OFFICE OF INFORMATION PRACTICES

STATE OF HAWAII

THE COMMERCIAL USE OF PERSONAL INFORMATION

DECEMBER 1999

ACKNOWLEDGEMENTS

The Office of Information Practices acknowledges the substantial contributions of the following in the research, development, and production of this report: the members of the public who contributed comments and ideas; the representatives of private businesses who participated in discussions and contributed information for the data flow questionnaire; representatives of Associated Credit Bureaus, Inc. (Washington, D.C.) and the Polk Company (Chandler, Arizona), who traveled to Hawaii to discuss issues; the various privacy regulators, academics and consultants from the Asia-Pacific region, Canada, Europe, and the U.S. mainland who provided detailed responses to our inquiries and participated in discussions; the Hawaii State Legislature, for assistance and providing facilities for the hearing; and the Office of Information Practices staff, for support services.

The Office of Information Practices has been monitoring the development of informational privacy as part of its administration of public sector information practices. Much of Mr. Hester's work during his law school internship with this office focused on the issues relating to the privacy of information in the private sector. Substantial portions of Mr. Hester's writings are included in this report.

Authors:

Moya T. Davenport Gray, Director
Office of Information Practices

John E. Cole, Staff Attorney
Office of Information Practices

Jeff Hester, Esq.
Reinwald, O'Connor & Playdon

Lisa Asato, Student Intern
Office of Information Practices

This report to the Legislature is pursuant to House Concurrent Resolution 196 and House Resolution 180 (adopted April 1999).

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The use of personal information in traditional commercial settings is pervasive. Electronic commerce, especially the use of the Internet, will increase the globalization of goods, services, labor and transactions, and all the personal information resulting from those events. But concerns about informational privacy arising from electronic commerce will dissuade consumers from the using the Internet to buy goods and services.

In the 1970's the concern was clearly about government's collection and use of personal information. Today, however, the concern is with the private sector. The private sector is now the largest user of personal information and there are no standards governing the private sector's handling of personal information. The rise of an information economy has removed the control of personal information from the hands of those to whom it pertains, and who have the highest stake in the information remaining confidential, and put it into the hands of businesses and industries that thrive from sale and purchase of informational products.

Without clear standards to protect personal information, Hawaii will not benefit from electronic commerce and will fall behind. Hawaii already has an informational practices scheme in place which provides privacy protection for personal information in government records. The Uniform Information Practices Act (Modified) ("UIPA") §92F (1988), as it was intended to, covers only information held by government agencies. This study recommends that the State of Hawaii extend its privacy protection scheme to personal information held by the private sector. However, such a privacy protection scheme must be tempered by several considerations.

First, electronic commerce is in its infancy; its capacity to generate products and services are being developed daily. Standards that are too rigorous would likely stop innovation. Thus, statutory standards and protections should, where possible, encourage the growth and stability of "e-commerce" and should not unduly hamper its growth.

Second, the American regulatory landscape that applies at the federal and state level creates an obscure environment for both consumers and businesses. Therefore, statutory standards and protections should reduce the uncertainty and risk to both the consumer and business.

Third, as government's resources are limited, they should not be used to micro-manage the private sector's use of personal information. Nevertheless, it is critical that clear standards be enforced. Government and industry must be able to work together to produce the desired result. Therefore, a statutory scheme should:

1. reduce excessive government control and involvement in the flow of personal information, and empower a one-on-one relationship

between the consumer and the collector of information in which the consumer controls the flow of information;

2. provide for codes of practice that are meaningful for individual participation in this electronic society to be developed by government using the expertise of the private sector;

3. minimize government's role where the private sector has the capacity to enforce the standards. Where the private sector does not have or is unwilling to provide the capacity, then government will take an active role in enforcement; and

4. as information will undoubtedly involve transborder transfers, provide for the government's a role in ensuring that its standards are respected and followed.

The Office of Information Practices recommends that legislation, as set forth in Appendix A, be adopted.

INTRODUCTION

Globalization of the world's economies ties each of us to each other, no matter where we live.[1] Events in one country impact other countries in ways that have never been experienced before. Globalization affects more than a country's monetary concerns.

Electronic commerce will further spur globalization of sale of goods, services, labor, transactions, and all the associated personal information. With the growth of the Internet as a commercial market place, the globalization process will grow exponentially. Hawaii is quickly positioning itself to be part of that exponential growth.

However, a major obstacle to the growth of the Internet as a commercial market place is customer confidence.[2] At the June 1999 Asia-Pacific Economic Cooperation (also referred to as APEC) Electronic Commerce Steering Group Meeting held in Auckland, New Zealand, Bruce Slane, Privacy Commissioner for New Zealand, presented a paper in which he concluded that privacy concerns posed a barrier to the development of electronic commerce. Mr. Slane wrote:

> It is interesting to consider why, in a consumer age where quality, choice and convenience is demanded, the level of e-commerce is so low…. People are concerned about their rights and remedies when the goods or services are not up to the mark. They worry about the security of their personal information and fear it may be misused. Information privacy concerns are discouraging consumers from the using the Internet to buy goods and services.[3]

Mr. Slane reviewed surveys of American Internet users and found that they were concerned about their privacy, and specifically about surreptitious tracking of visits to websites, capturing of email addresses to be used for marketing without permission, posting of personally identified public records on the Internet, and reading of email addressed to someone else. Slane concluded that "a lack of privacy protection was deterring people from using the Internet and e-commerce." Surveys indicate that customers will not use the Internet as a market place unless their privacy is protected, their financial information is secure, and there are remedies in place to protect them as consumers.

Hawaii already has an informational practices scheme in place which provides privacy protection for personal information. However, the Uniform Information Practices Act (Modified) ("UIPA") §92F (1988) covers only information held by government agencies. When Hawaii's first fair information practices statute was enacted, people were concerned about government's use of personal information. Legislation across the United States of America targeted governments and the use of government-held personal information. Today however, the private sector is the largest user of

personal information and there are no standards governing the handling of personal information by the private sector.

Intuitively, people focus on privacy protections in the private sector because over the last twenty years the dramatic increase in the collection, use, and movement of information has eroded the concept of personal privacy in the United States.[4] The rise of an information economy has removed the control of personal information from the hands of those to whom it pertains, and who have the highest stake in the information remaining confidential, and put it into the hands of businesses and industries which thrive from sale and purchase of informational products produced from this information.[5] Personal information fuels an industry valued in the billions,[6] that is dependent upon the thorough tracking, monitoring, and recording of people's personal lives and interactions with society in order to create valuable databases of profiles of almost every household.[7]

In the United States, this information gathering occurs within an environment without clear, legally enforceable standards, and in which individuals have no meaningful control over their own information.[8] For the most part, there is nothing coercive about the collection of personal information because most people either divulge much of this information or are unaware that the information is being collected and used.[9] Certainly, one sees the benefit of having one's preferences catered to by businesses -- and this catering gives the business a better opportunity to sell its product.[10]

The consistent maintenance of these records, however, becomes invasive and the disclosure of this aggregate information reveals far more than most people would willingly communicate to unknown persons.[11] Significantly, individuals do not know that this information is collected nor how it is used - either by the collector or by the business that obtained it from the collector. Most individuals probably don't know that the same information can be used to trace their whereabouts and where they have lived for the past ten years, what kind of car they have driven and where that car is today. They probably don't know that visits to websites are now tracked and that data is given to anyone who wants it; that what they purchase is compiled into a profile and in some fashion used in ways not anticipated by the consumer; that parts of their medical records are sold to drug companies; or that they have been included in medical databases that are used by drug companies to sell drug or medical products.

The Office of Information Practices (OIP) concludes that, if it were generally known how information is subsequently used, Americans would not participate in a structure that did not protect their information, including the Internet. And yet, meaningful participation in many areas of society, especially the Internet, depends upon the mandatory exchange of information. Should there not be acceptable methods of participation, the only alternative is exclusion from the social benefit.[12] Inadvertent errors in use, misuse, or even abuse of personal information can have devastating results,[13] which illustrates why society needs legal protections of our privacy interest in personal information.

In 1980, the Organization for Economic Cooperation and Development (OECD) an international body comprised of 24 countries throughout the world, including the United States, issued Guidelines[14] to help "harmonize national privacy legislation and, while upholding human rights, [to] at the same time prevent interruptions in international flows of data. [The Guidelines] represent a consensus on basic principles which can be built into existing . . . legislation or serve as a basis for legislation in those countries which do not yet have it."[15]

In 1998, the European Union's Council Directive on the Protection of Personal Data[16] came into force and gave European Union Member States the power to restrict the flow of information to those countries that do not have adequate standards. In response to the European Union's directive, countries beyond Europe, particularly in the Asia-Pacific region, have recently begun making sweeping revisions to their domestic information policies. This development is of prime concern to Hawaii because of its location in the Pacific and its close economic ties to the Asia Pacific region.

The Asia Pacific model of personal information protection is based on the OECD Guidelines and provides for industry flexibility through the adoption of industry specific codes of practice. These codes of practice are drafted by the industry in conjunction with the government, and when adopted, replace the enacted privacy standards. [A further explanation of the OECD Guidelines, the EU Directive, and the Asia Pacific model is provided in Appendix B, *Uniform Standards to Protect the Privacy of Personal Information.*]

While the rest of the world is taking on these issues in earnest, industry, privacy advocates and government agencies in the United States have been caught up in arguments over whether there should or should not be government regulation in this area. While factions argue that the Internet should not be regulated, the lack of informational policies regarding privacy, financial security, and consumer protections, erode consumer confidence daily, and in turn, slow the growth of electronic commerce.

Hawaii has the primary elements in place to protect our budding information economy and to become part of the global marketplace, by ensuring that the scheme to protect the use of personal information in the commercial environment is clear, comprehensive and reduces the risk of uncertainty - for both the consumer and business. Taking advantage of the growth of electronic commerce requires an environment that will enhance electronic commerce. Enhancement includes many factors, including a legal framework that reduces uncertainty and risk without impeding the development of electronic commerce. Hawaii should extend its system of informational privacy beyond the public sector to ensure the integrity and continued flow of the world's most heavily traded commodity: information.

STUDY METHODOLOGY

The OIP was asked to assess the way in which information is collected and used by the private sector. As Hawaii adopted a medical records privacy law in 1999 (Act 87 Session Laws, 1999), no attempt was made to conduct an in-depth review of the use of personal information in the health care industry for purposes of this study.

To understand how personal information is used, the OIP wanted to track the "flow" of information from collection, to maintenance and use within an organization, to dissemination outside of the organization. The OIP also wanted to know to what extent the organization was under governmental constraints and regulation, whether local, federal, or international. To do this, the OIP developed a questionnaire to determine the manner in which data flowed within and between business sectors, and to elicit information about the data handling practices of individual businesses. The questionnaire posed a series of questions in several categories, including data use, regulation, collection, data processing and storage, use of data within a business, protection of data, disclosure to third parties, and openness and accountability. [The questionnaire is attached to this report as Appendix C.]

This questionnaire was given to over fifty local and mainland businesses. The OIP, however, received only *seven* completed questionnaires from local banks, Internet service providers, and a retail merchant. No insurance company provided answers to the questionnaire. The respondents' answers were similar. Because responses to the data flow questionnaire were so limited, the answers should not be considered representative of any particular business sector, but representative of those businesses that take the issue of privacy seriously. Other responses received by the OIP included written explanations of the federal and state laws regulating the businesses, and brochures and pamphlets explaining the businesses' data collection practices and privacy policies. One insurance industry representative provided the OIP with a brief on how medical information was used within the industry. Still other companies sent representatives to meet with representatives of OIP personally to discuss privacy issues and the business' practices regarding collection and use of consumer information. We are grateful for the efforts of those businesses that were willing to provide assistance to OIP in determining the current uses of information and to explain their data handling practices and privacy policies.

To receive comments and testimony on the commercial use of personal information, the OIP held public hearings at the State Capitol on October 29, 1999, and by videoconference to include the islands of Hawaii , Kauai, and Maui on November 2, 1999. The October 29 hearing was well attended by local business representatives, and included media coverage.

The OIP also conducted extensive research on the issues surrounding the privacy of personal information in the private sector at the local, national and international levels. In addition, the OIP consulted with various agencies of the state government, local, national, and international public interest groups, and academics, and government officials from around the world.

Part I of this study will set forth OIP's findings. Part II of this study will, using the Schwartz and Reidenberg model referred to in the Appendix, explore current privacy protections in state and federal law. It will explain why these approaches to this issue are inadequate. Part III of this study contains the OIP's recommendations. Following some of the recommendations of the Alliance for Global Business in its Global Action Plan For Electronic Commerce[17], the OIP proposes that legislation be adopted to enhance the growth of electronic commerce, and to provide the people of Hawaii with statutory protections that are meaningful in an electronically connected economy.

PART I:

PERSONAL INFORMATION AND USES IN THE COMMERCIAL ENVIRONMENT

SUMMARY OF PART I

This section sets forth OIP's findings as to how personal information is used in the commercial environment, reporting the results of OIP's questionnaire and discussions.

Our personal information has a commercial value far beyond the purpose for which it originally was given. Every time one surfs the Internet, one leaves a "data trail" that is sold to other companies. This data train can be combined or compiled with other readily available public and non-public information to provide a detailed record of personal histories, locations, transactions, and preferences. This information is sold or used without the person's knowledge or consent. The sale of customer information to marketers by a Minnesota bank[18], and the sale of pharmacy records to large pharmaceutical drug companies[19], are uses of personal information in ways that were never intended. These are just two recent examples that have raised public concern over the handling of personal information by private companies.

In Hawaii and throughout the rest of the United States, the private sector gathers and uses personal information without clear, legally enforceable standards, and individuals have no meaningful control over information about themselves. When personal information is collected and stored by traditional methods, i.e., paper-based methods, there is usually nothing coercive about the collection. Many people voluntarily provide some of this information. Certainly, there are many legitimate reasons for businesses to maintain financial and other personal information about their customers. Our economic system could not function without the collection of some consumer information.

However, when information is gathered electronically, it is often done surreptitiously. Or, information that was gathered in a traditional fashion is now being compiled with other data and used in ways never anticipated by the individual. The development of technology, of user-friendly databases, and the Internet have crystallized the concern over information privacy. With these tools we can assemble or correlate information on a selective basis to *create new personal information*. It is this combination of such information into profiles that becomes highly personal and invasive.

In addition to the use of information on paper, the commercial collection of personal information on the Internet has grown in an exponential fashion. Moreover, the placing of personal information on the Internet now allows profiles to be compiled without regard to the wishes of the individual. The resulting combination can prove to be deadly. Negligence, errors in use, misuse, or even abuse of personal information can have devastating results. However, because there are no uniform standards for collecting and using personal information, public concern over the this issue will continue to slow the development of e-commerce. A framework of uniform standards would not only protect the privacy of personal information, it would also promote consumer confidence

and trust by ensuring consistency and fairness in the way businesses collect and use information.

TRACKING THE FLOW OF PERSONAL INFORMATION

RESPONSES TO DATA FLOW QUESTIONNAIRE

COLLECTION OF PERSONAL INFORMATION

The respondents to the Data Flow Questionnaire all collected personal information for several legitimate business functions, including sales or marketing and for billing or collections. Most respondents also collected and used personal information for human resources purposes. Other areas of collections and use included financing, credit, insurance, customer service and technical support purposes.

The respondents typically rely upon electronic data processing and storage, to a greater extent than on the use of paper for processing and storing data. One respondent commented that "[i]t is safe to say the electronic data processing and storage will continue to become more prevalent and paper processing and storage less prevalent over time." All seven of the respondents indicated that they use personal information that is received from outside the U.S. or transmitted to foreign countries minimally, if at all. One respondent indicated it did have difficulty transferring data between the Hawaii offices and its international offices in the Pacific because of governmental regulations related to privacy.

All respondents collect names, home addresses and home telephone numbers. The retail merchant and the banks also collect social security number, age, income, and (except for one bank) ethnicity. Most of this collection of personal information is directly from the person to whom it pertains, but many of the respondents indicated they also use secondary sources of personal information, as well as electronic tracking methods to obtain personal information. At least two of the respondents indicated they do not advise customers of their collection practices when obtaining information about them from an electronic tracking source. While most respondents generally advise people that they are collecting information about them, how the information will be used, and that they may choose not to have their information used in particular ways, one respondent indicated they did not provide any of this information.

DATA PROCESSING AND STORAGE OF PERSONAL INFORMATION

All respondents process data in-house, and several also use an outside vendor or contractor. Those respondents that do use outside contractors stated that they include confidentiality clauses in the agreements and prohibit the sale or reuse of customer information by contract. There do not appear to be remedies available to the individual if an outside vendor breaches the contract. The length of time personal information is kept by the respondents varies, with the longest being seven years.

USE OF PERSONAL INFORMATION WITHIN BUSINESS

All respondents indicated that within their organization, access to personal information is restricted to persons with a business need to know. While most respondents defined "business need to know" similarly, one respondent gave the far broader statement that personal information is that which is necessary "to adequately serve the customers." Information is sometimes shared with affiliated companies, but those respondents, which follow this practice, allow the customer to opt-out of this sharing.

PROTECTION OF PERSONAL INFORMATION

All respondents indicated that personal information is protected against risks such as loss and unauthorized access. Methods of protection varied from locking papers and computer discs in cabinets at night, to the use of passwords and secure network servers, to fire walls and encryption software. All respondents also reported that employees, agents, contractors and temporary employees are educated about the protection of information. Most of the training is periodic, recurring at lengths of time varying from two years to every quarter.

DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES

Almost half of the respondents reported that they share personal information or customer data with third parties, but none sell, rent, or lease it. Those who do share such information provide their customers the opportunity to opt-out of such sharing, and do restrict the use or disclosure of the information by the third party, typically by contract.

OPENNESS AND ACCOUNTABILITY

One respondent indicated that its personal information practices and policies were not made available to the public. The rest of the respondents do make these policies available. Some are provided in pamphlets mailed to customers or available at the place of business, some respondents also make them available on their web sites. All but two respondents reported that individuals are able to access and correct any personal information maintained by their company about that individual. All companies reported that they have a designated person who is responsible for compliance with their information practice policies and for handling complaints.

REGULATION

All of the banks responding to the questionnaire stated that they were subject to several federal laws regulating their industry, including the Right to Financial Privacy Act, the Fair Credit Reporting Act, the recently enacted Financial Services Modernization Act (all discussed in Part III of this Report). Credit bureaus are also subject to federal regulation.

Representatives from one bank asserted that they prefer no additional regulation or to wanted such regulation to be delayed until federal laws were clarified. One of the Internet Service Providers commented that it employs a practice that is stricter than

federal laws because "current federal privacy laws are inadequate to address electronic privacy."

DISCUSSIONS WITH THE PRIVATE SECTOR

ASSOCIATED CREDIT BUREAUS, INC. AND CREDIT REPORT DATA

Associated Credit Bureaus, Inc. ("ACB"), represents, among others, credit and mortgage reporting companies, and individual reference service companies, all of whom generate, use, or provide informational products from credit reports and credit header data. Representatives of ACB traveled to Hawaii to meet with OIP and discuss privacy issues. ACB's clients collect both public and non-public record data. Non-public record data is collected from consumer-business transactions in the retail industry, from banks or other financial institutions, directory information sources, and product registration/warranty information.

The credit reporting companies are regulated under the Fair Credit Reporting Act and provide credit reports to those who are authorized under the Act to receive these reports. The Federal Trade Commission governs these entities. These entities also sell "credit-header" data to other groups, such as the individual reference service companies.

The individual reference service companies provide locator data to consumers, professionals and law enforcement officials who are trying to locate individuals. Credit-header data may include no social security number, parts of the social security number or all of the social security number. It may also include an individual's places of residence over a duration of time, and the month and day of birth.

Credit-header data may also be sold to financial service industries, direct marketers and other industries that want to be able to target the sales of their products.

SELF-REGULATION

ACB asserted its members are self-regulating in that the personal information its members collect, use, and disclose is already governed by industry standards of data protections. The ACB offered two examples -- the Direct Marketing Association's (DMA) Privacy Promise, and the Individual Reference Services Group's ("IRSG") Self-Regulatory Principles governing the dissemination and use of personal data.

DMA'S PRIVACY PROMISE: Members of DMA who engage in business-to-consumer marketing must agree to give notice that customers have a choice not to have their contact information rented, sold, or exchanged. All consumer marketers must honor individual requests to opt out of the sale, rental, or exchange of their contact information for marketing purposes. Those individuals who do opt out of the sale, rental, or exchange of their contact information for marketing purposes, are placed on a list that must be used before soliciting prospects so that the individual's choice not to receive solicitations is respected.[20] The DMA's Privacy Promise does not provide consumers with access to

information maintained about them, nor does it provide remedies, if information is used against consumers' wishes.

IRSG PRINCIPLES: The IRSG has fourteen members including all three national credit reporting systems, Equifax, Experian, and Trans Union. IRSG members offer commercial services to help identify, verify, or locate individuals, and often play a role in facilitating law enforcement, fraud prevention and detection, and a range of business transactions and legal proceedings. In 1997 all IRSG members pledged to adopt self-regulatory principles governing the dissemination and use of personal data, and to subject themselves to independent audits to verify their compliance with the principles.[21] Unfortunately, these audits are not always made available to the public.

The IRSG developed the principles as a result of the Federal Trade Commission (FTC)'s examination of privacy concerns and the uses of personal information from the sale of "headers" of credit reports. The FTC and the IRSG worked together to draft these principles. According to the representatives of IRSG, the FTC has taken the position that a violation of the IRSG privacy principles is a violation of the Federal Trade Commission Act as a deceptive business practice. The industry claims that this essentially gives oversight and enforcement of the IRSG privacy principles to the FTC.

The IRSG principles allow for varying levels of disclosure of personal information depending on the user and the purpose for which the information will be used. These are divided into three groups:

- "Qualified subscribers" have unrestricted access and are usually law enforcement officials.

- "Commercial and Professional" users are not allowed access to credit, financial, or medical records, nor mother's maiden name. They are allowed social security numbers and birth information when it is truncated; that is the birth year is not disclosed and neither are the last four digits of a social security number. This group of users includes some businesses, lawyers, prosecutors, and others; typical uses of the information include the locating of debtors, witnesses and suspects. To be included in this group, users must be bona fide professionals; there is no clear definition of a bona fide professional.

- All Other Users: The third group includes every one else. Most of the users in this third group are direct marketers. Thus, IRSG members may distribute personal information to any user if it does not knowingly include information that reflects one's social security number, mother's maiden name, non-published telephone number, or non-published address, credit, financial and medical records, among other things.

The IRSG principles do not provide individuals access to information maintained about them. When the IRSG members were asked about this, they replied that access is not always cost effective, because of the way in which data is stored in engineered databases. Therefore, access was not addressed in the principles.

An advocate for government enactment of privacy principles responded that claims that such access rights are too costly for business are bogus. Freedom of information laws have always had provisions that impose fees for unusually costly searches.[22] Another advocate commented, "Let us not fall into the trap of re-writing principles to accommodate technology, rather than the other way around."[23]

THE POLK COMPANY

The OIP also had discussions with a representative from The Polk Company, which collects and contractually sells motor vehicle data and statistics for vehicle recalls, demographic, product development research, and impact studies. If names and addresses are requested, they are given provided that the state law from which it was collected permits such disclosures. Hawaii releases some data for use in vehicle recalls, but the release of data for marketing is not allowed.

The Polk Company representative believes that it relies on public record information from a single source in each state (the Motor Vehicle Registry), it is forced to be a good steward of that information. If it is misused, it believe its access to the information would be eliminated.

The Polk Company representative stated that a benefit can be obtained from the use of personal information, but there must be a balance between privacy and legitimate uses. As an example, he cited CARFAX, a vehicle history service offered by The Polk Company. The Polk Company claims the use of personal information is beneficial because car owners and potential car buyers can research a car's history based on its Vehicle Identification Number. Any damage not reported to the buyer (e.g., flood, accident, odometer tampering) is then provided and can save consumers from buying vehicles with hidden problems or damage.

The Polk Company representative was not against government regulation in the area of business use of personal information. He felt it would further legitimize his company's use of such information.

INDIVIDUALS AT PUBLIC HEARINGS

Common Cause Hawaii voiced concern about the perceived one-sided manner in which businesses use personal information. It was recommended by Common Cause that a property right be created in personal information and that businesses should pay a fee for the use of such information, with market advantages given to those businesses that refrain from exchanging personal information. Common Cause Hawaii testified that

while businesses espouse capitalism for themselves, they espouse socialism for consumers.

Another testifier looked up his "author's biography" on a web site that offered his book for sale. He was surprised to find the biography attached to the book he had written described someone else. He stated that although this instance of misuse of personal information may be funny, it could be "dark in other cases." He felt that this might be a sign of the larger size and potential of problems of privacy.

A law professor testified that consumers should not have to "opt out," of the use of their personal information. Instead, consumers should be told that information would be used to contact them to sell products and be shared with third parties. He personally faced privacy infringement when, without his knowledge or consent, a local hotel had photographers take pictures of his minor child at the hotel's "Kid's Club" service, and publish it in a Japanese travel guide. Publication of such photograph was disturbing to the family. In response to the testifier's call for an explanation, the hotel said it had overlooked "simple courtesy" of seeking consent.

The same testifier also told of a similar misuse of personal information at a local hospital. After his child was born, he refused a newborn photography service offered by a company who had contracted with the hospital. However, the hospital refused to let the infant check out without a photo being taken, alleging that the photo was used as part of the identification process. The testifier begrudgingly complied and sternly expressed that he did not want to receive any offers to buy copies of the photograph or any other products. To determine whether would the hospital would comply with his requests, he filled out a form with his office address and his wife's name. A few weeks later, his wife was flooded with baby product solicitations addressed to his office, in addition to an offer to purchase the photograph taken of the child. The solicitations continued despite several strong requests to the hospital and the photography company to rectify the matter.

Another testifier related that certain medical records had been requested in litigation. However, the hospital disclosed more records than had been requested. Although the testifier tried to retrieve these "excess" records, he has been unsuccessful. These records were improperly passed on to attorneys and others. The case is closed, and his records are still out there in some unprotected fashion.

State Representative Ed Case testified that there is particular need to: 1) clarify the definition of "information privacy;" 2) dispense with the debate on whether informational privacy is covered in the Constitutional right to privacy – because citizens do have such a right; 3) focus on how to implement that right; 4) distinguish between legitimate use of information versus purely profitable use, and determine to what extent the latter occurs; 5) focus on truly informed consent; 6) not wait for the federal government to act in this area; and 7) listen to the concerns of consumers.

SURVEYS

In April of 1998, a survey conducted by Dr. Alan Westin, the publisher and editor of Privacy & American Business, an activity of the Center for Social & Legal Research, found that sixty percent of those using the Internet "do not think that business incentives to foster e-commerce will be enough to stimulate good privacy practices, and that legislation and legal enforcement will be needed."[24] The survey confirmed that privacy is very important to Internet users.[25] Nearly three out of four indicated it would be "very serious" to them if, among other things, web site visits were tracked surreptitiously, or personally identified public information was made available on the web.[26]

Another survey by Jupiter Communications found that sixty-four percent of respondents don't trust a web site even if its privacy policy is posted.[27] Still another survey by NFO Interactive found that the handling of consumer's personal information online was the main factor why people choose not to shop online.[28] Respondents stated that the "attribute that would most entice them to shop at a web site was 'trust that the site would keep personal information private.'"[29]

Concerns about their privacy deter most consumers from using the Internet for shopping. If such concerns could be allayed by ensuring that businesses followed basic information privacy principles, the full potential for the growth of e-commerce could be realized.

IMPACT OF TECHNOLOGY ON INFORMATION AVAILABILITY

The development of computer technology and the capacity to digitize information, the widely available personal computer, user-friendly databases, and the Internet have crystallized the concern over information privacy. The fear of what has been termed 'electronic surveillance'[30] is liberally chronicled in commentaries on data protection. Professor Colin J. Bennett states[31] that because computers have

> the ability to assemble information selectively, or to correlate existing information, [this is]… functionally equivalent to the ability to create new information. This capacity, obviously facilitated by information technology, enables agencies to identify, target, and perhaps manipulate a certain segment of the population that has common background characteristics.

Technology allows us to collect separate bits of information about a person, not ordinarily considered 'private', and use this information to create highly detailed 'profiles'[32] of a person's medical, financial, transactional or political history. It is this combination of such information into personal profiles that is invasive.

In the Information Age, virtually every piece of personal information concerning an individual is collected, stored and compiled. Every industry now collects and compiles as much personal information as is possible. Medical information is encouraged to flow through the use of electronic means. As a result medical record information is actively sought for a variety of reasons which include direct marketing of specialized medical products, health insurance purposes, employer-managed health care programs and scientific statistical information.[33] Financial institutions rely heavily upon personal information to create financial products, and collect the information through loan and product sales information and transactional data.[34] Retailers also rely upon consumer's purchase profiles, which are compiled from information collected at every purchase, whether in a department store, restaurant, grocery store, website, or from a catalog.[35] Public records about real property owners, motor vehicle registrations, driver's licenses and other government databases are compiled with other items of personal information obtained in the transactions above and used by the private sector.[36]

The large-scale commercial use of database technology, the growth of home computing, and increasing use of the Internet have dramatically altered business practices globally. This development of electronic technologies, accompanied by the present push for the development of more electronic commerce, has serious consequences for individual privacy. As one commentator has noted, "the inherent inefficiency of manual filing systems was quite an effective privacy protection until recent advances in automatic data processing."[37] However, today computers "hold half a billion bank accounts, half a billion credit card accounts, hundred of millions of mortgages and

retirement funds and medical claims and more. The Web seamlessly links it all together."[38] This compilation and combination of personal information is "a salesman's dream -- and a paranoid's nightmare."[39]

PERSONAL INFORMATION USE ON THE INTERNET

In addition to the commercial use of information by traditional methods, the commercial use of personal information on the Internet has grown in an exponential fashion. Media attention given to the ease with which personal information can be collected and used has recently swelled. Much of it has focused on the use of the Internet as the means by which data is found and the potential uses and abuses of information collected both with and without a person's knowledge. For example, a recent newspaper article describes how a web master can know what web browser you're using, and "may know where you live, the company you work for and even your e-mail address -- before you've done anything but click."[40] The article further states that in the near future, that same web master "might also know your name, social security number and occupation, how much you make, what kind of car you drive and how much you spent on clothes last year."[41]

Already, hundreds of "data detectives" have set up shop on the Internet, ready to fulfill almost any request for personal data to whoever will pay the price.[42] Web detective Daniel Cohn of Docusearch was challenged to find Forbes magazine editor Adam Penenberg's personal information, starting only with his byline. In six days, using only the Web and a phone, Cohn found Penenberg's two unlisted phone numbers, bank account numbers and balances, salary, rent, phone records, his favorite restaurant, and the fact that he pays about $700 a month to a psychotherapist.[43]

Docusearch also supplied 21-year-old Liam Youens with location data information - allegedly a social security number - about Amy Boyer, which was used to locate her. Apparently Youens had come into extended contact with Boyer only as a student, but held a disturbing fascination for her.[44] On October 15, 1999, Youens waited outside Boyer's New Hampshire office building, killed her, and then committed suicide.[45] Docusearch did nothing illegal. People have long been able to put together a profile from publicly available documents. As long as a person pays the fee, companies like Docusearch can provide such information with little difficulty.[46]

Some Internet companies also do their own detective work on the web. A class-action suit was recently filed in Federal Court in Pennsylvania against RealNetworks. The plaintiffs accused RealNetworks of assigning identifiers to the user of its RealJukebox software and, without letting the user know, compiling information about the users' music listening habits as they downloaded music on the Internet.[47]

SUMMARY & FINDINGS

Personal information is collected everywhere. Retail transactional and financial information is collected at the supermarket, department store, boutique, gasoline pump or other shop at which a consumer pays for the goods or services by check, credit or debit card. Medical information is collected at every point at which a person has contact with any portion of the vast and pervasive health care industry. Medical information is collected when a person applies for life or other insurance coverage or when your child begins school. Gender information is collected almost everywhere you turn. Religious information continues to be collected by the health care and travel industries. Educational information is collected by educational institutions, but it is also collected by both permanent and temporary employers. Tellers and clerk, securities brokers, mortgage brokers, and insurance agents collect financial information. Along with other financial information, bankruptcies and civil actions are collected and published by local newspapers. Marital status, social security numbers, current address, emergency contacts, immunization and other medical information, are collected for participation in any sport, job application, credit card application, loan application, brokerage account application.

Personal information is used throughout the private sector for commercial purposes. Retail transactional and financial information is utilized for consumer profiling, and is reported to the credit reporting agencies. Credit reporting agencies then share portions of that personal information with paying clients, including locator services and direct marketing services. This same information is then used to locate persons and to sell products to people. Medical information is disclosed to a national database when a person applies for life or other insurance coverage or to the government when your child begins school. Medical information is disclosed to persons outside the health care industry when a claim for damages is made either through such statutory schemes as worker's compensation or through insurance claims. Gender and lifestyle information and religious affiliations are shared in hospital and clinical settings and travel industries. Website profiles are created for the advertising industry and are obtained by government agencies.

The OIP concludes that the commercial use of personal information is pervasive; that the collection and use of information is considered proprietary to the collecting business; that some businesses take some steps to protect privacy, but others do not. In fact, some businesses appear to actively invade privacy for the sake of profit. The OIP also concludes that people want to control how their personal information is used and have their wishes complied with when expressed. Even the many people who enjoy getting catalogs and having buying choices tailored to their specific preferences feel they should have the right to say no and to be able to restrict the flow of their personal information. Particularly, with the increase in database and Internet use, many people feel that any control they may have had over their information is slipping away.

PART II:

THE UNITED STATES OF AMERICA:

A PATCHWORK APPROACH TO PROTECTING PRIVACY

SUMMARY OF PART II

Professors Schwartz and Reidenberg, in their book entitled *Data Privacy Law*, suggest that there are four main elements that are necessary for the protection of personal information in the private sector. They are:

- the establishment of obligations and responsibilities[48];
- the open or transparent processing of personal information[49];
- the creation of a special category of "sensitive" data afforded the highest protection[50]; and finally
- the establishment of an enforceable remedy with oversight by an independent agency.

This section examines, in light of the Schwartz and Reidenberg model,[51] what protection is afforded the personal information of an individual on the national and state levels.

GOVERNMENT RECORDS: THE FEDERAL PRIVACY ACT OF 1974. In general, the privacy act restricts the collection, use and dissemination of personal information by federal agencies, and assigns oversight to the Office of Management and Budget.

PRIVATE SECTOR LEGISLATION. Despite the growth of information technology, the United States has not enacted comprehensive privacy legislation on a national level beyond the Privacy Act of 1974. Those pieces of legislation that do touch on privacy do so in a problem-specific manner; thus, as technology or industry changes, the law becomes ineffective. The private sector has not been required to implement legally enforceable fair information practices. Unfortunately, this void leaves individuals virtually defenseless in a society that demands participation through the exchange of information. Currently there are no omnibus bills dealing with the commercial use of personal information before Congress.

HAWAII AND OTHER STATES: Hawaii has three essential components for the fair treatment of personal information: a constitutional right, comprehensive protection of government records, and a monitoring agency, the Office of Information Practices. It does not, however, have any uniform legislation that governs the treatment of personal information in the private sector. This combination gives Hawaii the most comprehensive system of informational privacy of any state. The interplay between these components contributes significantly to the elements making up the developing international model of protection for personal information. Other states have constitutional rights to privacy but have not adopted omnibus privacy protections.

SELF REGULATION: In cases of self-regulation by industries through the establishment of internal codes of conduct the problem has always been enforcement. Self-regulation of personal information on the Internet seems to have failed.

Federal Legislation

Ironically, the United States was considered the world leader in privacy during the period of international study concerning this issue.[52] As the first nation to implement an innovative and comprehensive set of rules, the United States for some time provided an example after which other nations modeled themselves.[53] The Privacy Act of 1974[54] was the starting point and marked the pinnacle of the United States' leadership role in safeguarding the personal information of its citizens.

GOVERNMENT RECORDS: THE PRIVACY ACT OF 1974

In the wake of the Watergate affair, Congress as a policy response to misuse of personal information passed the Privacy Act of 1974 by the Nixon administration. The Act had origins similar to the developments which led to comparable legislation passed in Europe,[55] but the Watergate scandal lent credence to the types of misuse possible in an increasingly information driven society.

In general, the Privacy Act restricts the collection, use and dissemination of personal information by federal agencies, and assigns oversight to the Office of Management and Budget (OMB). Overall, the Act represents a reasonably comprehensive attempt towards fulfillment of the first element of the data protection model;[56] however, it has several important limitations that hinder its overall effectiveness.

The largest criticism of the Privacy Act of 1974 is the abuse of so-called routine use exemptions.[57] This exemption allows an agency to disclose personal information without the consent of the individual.[58] Despite widespread and vocal criticism, the practice continues virtually unabated due to the limitation of remedies available to individuals through the court.[59] This leaves individuals practically powerless over which federal agencies are receiving personal information about them.

Although the federal statute provides for a notice of how that information would be used, one questions how truly transparent this method is because individuals are put on "notice" through the use of a broad statement that fails to explicitly indicate how the information will be used. Notice is given through a listing in the Federal Register providing constructive notice at best and leaving individuals unaware of when or where their personal information is being used.[60] Moreover, protecting sensitive data[61] is effectively destroyed by an over-used law enforcement exception, which again allows data to flow freely among agencies.[62] One commentator believes that the element of oversight is lacking, despite the existence of the OMB, because of the loose interpretation of the routine use exemption.[63]

As further evidence of the United States' information policy, the Privacy Act of 1974 does not regulate how a federal agency may acquire information, only how such

information is treated once under agency control.[64] This system cannot foster fair information practices when the federal government, supposedly restricted in its information practices, can acquire massive amounts of unregulated personal data collected from private companies in addition to that information it collects directly from the individual.

Overall, the Privacy Act of 1974 does address each of the four elements of a data protection model[65]; however, the existence of significant loopholes undermine the benefits individuals supposedly receive.

PRIVATE SECTOR LEGISLATION

Despite the growth of information technology, the United States has not enacted comprehensive privacy legislation on a national level beyond the Privacy Act of 1974. Rather, Congress has implemented a wide variety of very narrow legal rules which target specific problems.[66] The result is that an individual's privacy protection depends entirely upon the rules for that one sector. Under the federal approach, personal information is treated differently depending upon the context, and the associated enforcement mechanisms for individuals can vary for almost identical violations. This ad hoc approach creates overlap in certain areas and leaves gaps in others, often leading to results which muddy the waters, rather than creating certainty.[67] More importantly, this approach cannot keep pace with technological and industry developments.

THE FAIR CREDIT REPORTING ACT OF 1970 (FCRA)

The Fair Credit Reporting Act 1970 (FCRA) regulates the collection and use of very specific items of consumer credit information and assigns specific rights to individuals.[68] The FRCA most closely resembles the European model of protecting the processing of personal information. However, the protection it provides for personal privacy is at most dubious and limited only to specific items of credit information.[69] The FRCA defines how credit information is disseminated, who can receive such information, and provides a mechanism for individuals to check the accuracy and completeness of their record.[70]

While the FCRA does provide some protections for the individual, it does not regulate how credit information is collected and relies, primarily, upon the individual to discover inaccuracies. Although the FCRA has been criticized for broad language and vague drafting[71], the 1998 amendments attempted to eliminate some of these faults.[72] The FCRA lists the permissible purposes for using consumer reports. They include in response to a court order, at the instruction of the consumer, to a person the consumer reporting agency has reason to believe intends to use the information to extend credit, for employment purposes, insurance underwriting, to determine eligibility for a license or benefit, and to assess credit risk.

THE FINANCIAL SERVICES MODERNIZATION ACT

President Clinton signed the Gramm-Leach-Bliley Act, also known as The Financial Services Modernization Act ("FSMA"), into law on November 12, 1999. The FRCA removes depression-era restrictions on bank holding companies. Now, in addition to traditional banking services, banks may engage in insurance, underwriting, investment, and securities activities, and may acquire companies that perform these services.[73] As the FSMA eliminates the "walls" between traditionally separate sectors of business, the authors anticipate that the sharing and use of personal information between these sectors of business will increase drastically.

Congress has now allowed these disparate industries to change their shape to allow the banking industry to compete with other "financial services" under the guise of consumer convenience. But the danger to personal information is that these newly shaped financial service companies can collect and transmit personal information from one affiliate to another without clear standards that protect consumers.

While proponents of FSMA point out the privacy protections in the bill, the OIP does not see clear standards in the bill and believes that Congress has created an impossible task by assigning eight federal agencies the job of creating these standards. While these federal agencies have five months to develop privacy standards under this Act, the banking industry reports that it is likely that turf battles will accompany the process of rule writing. The industry reports that some people expect the five-month deadline to be extended.[74] This environment is not conducive to the creation of standards that will protect consumers in a consistent and comprehensive fashion.

THE VIDEO PRIVACY PROTECTION ACT

The Video Privacy Protection Act[75] is the most notable example of targeted legislation to address a specific problem. This law protects the video rental records of customers in response to the disclosure of Judge Bork's video rental records during his Supreme Court nomination.[76] The Act applies only to rental records for videos, leaving to Congress the task of passing legislation to cover other records relating to home entertainment.[77]

RIGHT TO FINANCIAL PRIVACY ACT OF 1978

The Right To Financial Privacy Act[78] ("RFPA") restricts only the government's ability to obtain to financial records. It prohibits access by Government authorities, except under certain circumstances, including consent, subpoenas, and search warrants. The RFPA also prohibits release of records by financial institutions to any Government authority except in accordance with the provisions of the chapter.[79]

THE FEDERAL TRADE COMMISSION ACT

The Federal Trade Commission Act[80] ("FTCA") requires each federal supervisory agency to establish a separate division of consumer affairs to handle consumer complaints regarding unfair or deceptive acts or practices. In addition to complaints

regarding violations of existing law, a complaint can be directed at an act or practice even if it is expressly authorized or prohibited by current law. In conjunction with other federal laws, the FTCA can be used to enforce an institution's disclosed privacy principles, because non-compliance with the disclosed principles can be considered a deceptive act.[81]

CHILDREN'S ON-LINE PRIVACY PROTECTION ACT OF 1999

The Children's On-Line Privacy Protection Act[82] ("COPPA") is the only federal legislation that specifically addresses personal information collection on the Internet. It provides that web sites must have verifiable parental consent before collecting, using or disclosing personal information about children. Violations of regulations prescribed under the Act are treated as an unfair or deceptive act or practice under the Federal Trade Commission Act.

In late April, the FTC issued its proposed regulations to implement the COPPA. Under the proposed rules, web sites that target children must obtain parental consent before collecting personal information from children under age thirteen. Parents will also have the right to decide whether information about their children may be disclosed to third parties and to prohibit future use and collection of information about their children.

Conspicuously absent from this brief survey is legislation relating to medical privacy. The lack of protections in this area has provided some of the most egregious examples of misuse of personal information.[83] At present, however, the reality is that despite high public concern over the issue Congress has not passed legislation to protect a person's medical information; this information is less protected than his credit records, cable records, and video rental records.

The national picture provides a confusing multitude of laws protecting various aspects of personal privacy. These laws are primarily concerned with limiting government activity, and rely upon the public to monitor information practices. The private sector has not been effectively obligated to implement legally enforceable fair information practices, leaving individuals practically defenseless in a society that demands participation through the exchange of information.[84] The data protection scheme of the United States is incomplete and varies according to sector.

With this fragmented approach, effective oversight at the national level is lacking.[85] Citizens have no effective protection from abuses. Currently there are no omnibus bills dealing with the commercial use of personal information before Congress. The Federal Trade Commission has repeatedly warned the private sector to be effective at self-regulation or it will take steps to regulate. To date, it has not. These ills, which many believe would be more appropriately addressed on a national level, can be more effectively controlled on the smaller scale of the state where citizen's voices are readily heard.

STATE EFFORTS

States have, in general, taken the same piecemeal approach to privacy that the federal government has taken. There is a great deal of confusion and disarray at the state level,[86] and only a handful of states have attempted to address this issue comprehensively.[87] Other states have constitutional rights to privacy but have not adopted omnibus privacy protections.

States that have attempted to address informational privacy issues with comprehensive legislation introduced in 1999 include California (Senate Bill 129) and Texas (House Bill 611). A weak version of the California bill awaits conference committee consideration. The Texas bill died during the 1999 session, but an interim committee, Chaired by Representative Kyle Janek, has been assigned to study privacy issues, including the effects privacy legislation would have on sharing of information between affiliates of large corporations. The interim committee is to work with all interested parties and attempt to reach a consensus on what type of privacy protections are reasonable. The committee will begin work in January 2000, and Representative Janek hopes that new privacy legislation will be introduced at the next session in January, 2001.

Additionally, the State of Washington Attorney General has organized a Consumer Privacy Workgroup to look into consumer privacy issues and make recommendations to strengthen privacy protections. The workgroup is comprised of consumers, business leaders, information experts, and legislators, and holds regular public meetings to receive comment and input from the community. Just recently the State of Maryland proposed that state agencies be required to adopt fair information practice principles. Although businesses would not be covered by such a law, they would be encouraged to voluntarily adopt these same principles, and set up and manage an organization that would certify participating businesses and offer education to consumers.

STATE OF HAWAII

Hawaii already has three essential components for the fair treatment of personal information: a constitutional provision[88], comprehensive legislation governing government records[89], and a monitoring agency.[90] It does not, however, have any uniform legislation that governs the treatment of personal information in the private sector.

THE CONSTITUTIONAL RIGHT TO INFORMATIONAL PRIVACY

The Hawaii State Constitution was amended in 1978 to include a "right to privacy" to be considered apart from the previous interpretation by the Hawaii Supreme Court limiting it to only criminal cases. [91] The new provision reads, "The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right."[92] This new right encompassed privacy in the informational and personal autonomy sense.[93] Specifically addressing the informational aspect of privacy the Standing Committee report states:

> There has been a trend in modern-day society to require that a person complete forms detailing information about himself. There is often a legitimate need for government or private parties to gather data about individuals, but there is a danger of abuse in the use and/or dissemination of such information. The danger of inclusion of inaccurate data being retained in some computer bank, thereby affecting the life of an individual, is inherent in our modern day, but the right to privacy should insure that at the least an individual shall have the right to inspect records to correct information about himself.[94]

In this report, the proponents of the added constitutional provision wanted this informational and personal autonomy form of privacy to be considered a fundamental right equal to First Amendment rights.[95]

APPLIES TO PRIVATE SECTOR:

The explicit connection between data protection and privacy is further bolstered by a mandate that this section be applicable to the actions of private parties. The Standing Committee Report to the Convention[96] states:

> Your Committee recognizes that generally the Constitution acts as a safeguard against the actions of government and not private parties. Therefore, Your Committee has mandated that the legislature implement this section since statutory language can be legitimately drafted to protect against the actions of private parties.

Furthermore, the Committee of the Whole Report concluded, "Privacy as used in this sense concerns the possible abuses in the use of highly personal and intimate information in the hands of government or private parties but is not intended to deter the government from the legitimate compilation and dissemination of data."[97]

These provisions have been recently reinforced by the Hawaii Supreme Court in determining the limits of protection afforded by this constitutional right of privacy.[98] The Court previously interpreted informational privacy as the "right to keep confidential information which is highly personal and intimate."[99] It was the mandate of the Standing Committee to include private actors within the scope of this right[100] and they gave the Legislature an affirmative duty to implement this right.[101] The judicial recognition of these provisions is of utmost importance because the Hawaii State Legislature can constitutionally extend the protection of privacy in personal information to the private sector.

COMPREHENSIVE LEGISLATION REGARDING GOVERNMENT RECORDS

In 1988, Hawaii passed the Uniform Information Practices Act (Modified) (UIPA), an informational practices statutes which encompasses both freedom of information principles and privacy principles.[102] It uses a balancing test between individual privacy and public access with a predisposition towards disclosure except when disclosure is clearly an unwarranted invasion of privacy.[103]

All four elements of the Schwartz and Reidenberg model are present in the UIPA. However, because the UIPA's primary function is to set uniform policies regarding government records, the information practices principles are set forth in a different manner than in a straightforward privacy scheme.

Some of the obligations and responsibilities are not directly legislated, but are addressed as underlying policies of the Act .[104] For example, it is expected that the agency collect only that information which is "accurate, relevant, timely, and complete."[105] Additionally, secondary uses of personal information and data sharing between governmental agencies are legislatively limited.[106] Individuals do have access to their personal records except in five specific and narrow instances.[107] Moreover, an individual may correct his record or be given a prompt explanation of the refusal.[108] These provisions give individuals a powerful statutory right in personal information collected by government.[109]

The Schwartz and Reidenberg model requires that the processing of personal information be open or transparent. This element is accomplished in the UIPA by requiring each agency to set forth its policies and procedures and reporting to the OIP what types of records it keeps who in turn makes these reports public.[110] This method is akin to the European model of registration. Furthermore, OIP is charged with promulgating rules governing agency collection, processing, and disclosure of data, appeal procedures, time limits for action, and fees for accessing data.

The Schwartz and Reidenberg element of providing special protection for sensitive information is the strongest element of the Hawaii approach. The UIPA does not require disclosure of information that "would constitute a clearly unwarranted invasion of privacy."[111] The statute supplies representative examples of information in which an individual has a significant privacy interest including medical, financial and employment information.

INDEPENDENT OVERSIGHT

The final element in the Schwartz and Reidenberg model is that of establishing enforceable rights and independent oversight. Effective oversight of data protection is sorely lacking in a majority of states.[112] Hawaii's UIPA does both. As an independent government agency assigned to implement the UIPA, the OIP has oversight for the state's information practices.[113] The integral role of the monitoring agency becomes clear upon analyzing how Hawaii's informational privacy scheme operates in terms of the Schwartz and Reidenberg model, as shown above.[114]

In general, an oversight agency has three responsibilities: assistance to individuals, investigative and adjudicative authority, and the promulgation of rules and standards.[115] In assisting persons in the exercise of their rights under UIPA, the OIP will review and decide cases where agencies have denied access to information or improperly disclosed information.[116] The OIP also has broad investigative power to examine state agency records helping to keep government information practices as open as possible.[117] Lastly, the OIP is mandated to adopt rules governing agency collection practices, fees and appeals process, among others.[118]

With respect to establishing enforceable rights, the UIPA clearly provides for subject access to data and procedures for amending inaccuracies.[119] If an agency does not comply with these measures, the individual may appeal the agency decision to the OIP or directly to the circuit court.[120] If there is a dispute brought before the OIP, an investigation takes place and the OIP may issue a formal advisory opinion.[121] The agency is not bound by the OIP's decision but if appealed to court, the court may award actual damages, provide injunctive relief, and assess attorney's fees.[122]

The combination of a constitutional provision, fair information practices legislation and an oversight agency give Hawaii the most comprehensive system of informational privacy of any state.[123] The interplay between these components contributes significantly to the elements making up the developing international model of protection for personal information.[124] The result is a scheme of information practices that is capable of being extended to the private sector in order to meet the international standards.

SELF REGULATION

The economics of personal information are astonishingly lucrative. Sales revenue attributable to direct marketing in the U.S. is estimated to reach more than $1.5 trillion in 1999. By 2004, sales are estimated to grow by 8.8 percent annually to reach $2.3 trillion.[125] Advertising by direct marketers alone now represent 57.1 percent of the total U.S. advertising expenditure, and is projected to reach $308.9 billion in 1999.[126] Add these figure to the projected growth of electronic commerce via the Internet in the American, Asian and European continents and what you have is an overwhelming business incentive to collect and use personal information.

Prior to becoming President Clinton's Chief Counselor for Privacy[127], Peter Swire provided comments to the National Telecommunications and Information Administration (NTIA) dated December 23, 1996 and entitled "Markets, Self-Regulation and Government Enforcement in the Protection of Personal Information." As part of this study Mr. Swire reviewed the incentives for industry to regulate itself as to privacy. He wrote that "the incentives for industry to protect privacy are entirely financial" and noted that

> [t]he company gains the full benefit of using the information, notably in its own marketing efforts or in the fee it receives when it sells the information to third parties. The company, however does not suffer the full losses from disclosure of private information. Because of imperfect monitoring, customers often will not learn of that use. They will not be able to discipline the company efficiently in the marketplace for its less-than-optimal privacy practices.[128]

Mr. Swire found this situation to be a "systemic incentive to over-use private information."[129] It must be noted, however, that it is the use and disclosure of personal information, rather than its collection, that is most often objectionable, and thus the most threatening.

In cases of self-regulation by industries through the establishment of internal codes of conduct the problem has always been enforcement.[130] For example, self-regulation of personal information on the Internet seems to have failed.

Self-regulatory privacy seal programs attempt to include many aspects of fair information handling, but typically are ineffective because they have little power to enforce compliance. TRUSTe is an industry effort at self-regulation online. Companies can post its “TRUSTe” privacy seal after they have signed a contract agreeing to abide by certain privacy standards.[131] This seal is supposed to advise the web surfer that the website protects privacy. These programs are also used by only a small fraction of web sites, leaving the consumer to surf at his own risk through the majority of the Internet.

Further, privacy seal programs on the Internet can lead to a false sense of security--this is illustrated in the unfair trade practices complaint filed with the Federal Trade Commission against TRUSTe and America Online.[132] The complaint alleges that both TRUSTe and AOL claim that the seal program covers the "AOL.COM" web site. However, the seal covers only a small portion of the site, "www.aol.com," but not the members' area.[133] When a person visits www.aol.com they see the TRUSTe seal, but if they decide to join, they are transferred to the members area where personal information is collected and then released to telemarketers.[134] The Internet is an arena where the potential for the misuse of people's personal information is immense.

The class action suit against RealNetworks, is of special concern because the RealNetworks site displayed the TRUSTe privacy seal. TRUSTe has admitted it was powerless to do anything in the RealNetwork's case because the data was not transferred through the RealNetworks website, but by the software which was not covered by the seal.[135] While this is a technical and perhaps legally acceptable distinction, TRUSte's inability to prevent this violation of privacy indicates that self-regulation does not work.

While the RealNetwork's example is one that has made it to the courts, the secretive collection of information about web surfers continues. Advertising on the web is tailored to the web-surfer's profile. Tracking which websites a web surfer visits, all without the surfer's knowledge, provides the advertiser with information that is then used to send specific ads to the web surfer. Thus, a surfer's visits to medical, political, religious and lifestyles websites are all tracked and recorded, and if secret identifiers are added to software, the "profiles" can be identified to the software purchaser.

Although pure self-regulatory efforts are proceeding, they are not sufficient to protect the privacy of personal information. Unlike self-regulation, the cooperation between business and the overseeing authority in the development of these standards or codes of conduct can place accountability for fair information practices on each business and yet be tailored to fit the needs of a particular industry. While the standards may differ from industry to industry, an individual may still seek redress in a single agency, which simplifies the administrative procedure. This makes enforcement a realistic and achievable result.[136]

PART III:

RECOMMENDATIONS

RECOMMENDATIONS

The final part of this report sets forth our recommendations. Increasingly, businesses are finding that responsible data handling practices, including giving individuals control over the use of their information, is good for business.[137] The self-regulatory schemes in existence, or being developed today, include many aspects of fair information handling. However, the standards are inconsistent across sectors, and often lack meaningful methods of enforcement or complaint resolution.

A framework of uniform standards would not only protect the privacy of personal information, it would also promote consumer confidence and trust by ensuring consistency and fairness in the way businesses collect and use information. Consumer confidence and trust is important to all businesses, and essential to the development of e-commerce.[138] In conducting this study, three factors became very clear:

First, electronic commerce is in its infancy; its capacity to generate products and services is being developed daily. Standards that are too rigorous would likely stop innovation. Thus, statutory standards and protections should, where possible, encourage the growth and stability of "e-commerce" and should not unduly hamper its growth.

Second, the American regulatory landscape that applies at the federal and state level creates an obscure environment for both consumers and businesses. Therefore, statutory standards and protections should reduce the uncertainty and risk to both the consumer and business.

Third, as government has limited resources, government resources should not be used to micro-manage the private sector's use of personal information. Nevertheless, it is critical for the protection of both individuals and business that clear standards be enforced.

As noted by Peter Swire, it is "unlikely that either markets or government, acting alone, will do as good a job as we would like of achieving both privacy and other social goals such as efficiency."[139] Therefore, in any proposed scheme, government and industry must be able to work together to produce the desired result. The OIP believes that such a statutory scheme should:

- empower a one-on-one relationship between the consumer and the collector of information in which the consumer controls the flow of information. This reduces excessive government control and involvement in the flow of personal information used in the commercial setting;

- provide for the development codes of practice that are meaningful for individual participation in this electronic society to be developed using the expertise of the private sector;

- minimize government's role where the private sector has the capacity to enforce the standards. Where the private sector does not have or is unwilling to provide the capacity, then government should take an active role in enforcement; and

- As information will undoubtedly involve transborder transfers, provide for the government's a role in ensuring that its standards are respected and followed.[140]

The Alliance for Global Business in its Global Action Plan For Electronic Commerce noted:

> The protection of users, in particular with regard to privacy, confidentiality, anonymity and content control should be pursued through policies driven by choice, individual empowerment, industry-led solutions, *and…[in accord] with applicable laws* (emphasis added).[141]

Considering many recommendations by business, OIP's proposal defines acceptable behavior by setting standards accepted across the world and charges the individual with monitoring the actual practices of the respective industry; it provides a convenient forum for relief; and it balances the privacy interest of the individual with the interests of business and industry without impeding the free flow of information so necessary to our society. [A complete copy of the proposed legislation is attached as Appendix A.] Using the OIP's findings and the legislation introduced in the 1999[142] as guidelines, the OIP makes the following recommendations:

EXTEND INFORMATIONAL PRIVACY PROTECTION TO PRIVATE SECTOR

The OIP recommends that the State of Hawaii extend its statutory informational privacy scheme to cover the use of personal information in the private sector as was done in both H.B. 1232 and S.B. 991. The OIP recommends that the Asia-Pacific model be used as a foundation for such a scheme.

The privacy right recognized in section 6, Article 1 of the Hawaii State Constitution has been interpreted as applying to private parties as well as government.[143] Unlike the government, however, the private sector has no affirmative obligation to implement fair information practices.[144] Powerful private entities collect and compile information at a rate which rivals the public sector's collection and compilation.[145] Individuals should have rights to protect their personal information that is held by the private sector which are equal or similar to the rights to protect their personal information held by government. With no regulation, "the incentives for industry to protect privacy are entirely financial."[146]

Legislative recognition of this established Constitutional privacy interest cannot be said to unduly burden the private sector because it has been in force since the Constitution was amended in 1978. The legislation would simply require private actors to act affirmatively rather than avoid the current prohibitions on certain behavior.[147] Therefore, any effective extension of fair information practices into the private sector must necessarily begin with legislation that establishes a system of rights and obligations.[148]

ADOPT FAIR INFORMATION PRACTICES STANDARDS

As endorsed by the Alliance for Global Business,[149] the OIP recommends that fair information practice standards, based upon the 1980 OECD Guidelines, be adopted.[150] However, as the collection and use of information varies widely from industry to industry, comprehensive regulation may overburden some industries while being ineffective in others.[151] The Alliance for Global Business noted:

> Governments should adopt a flexible and responsive approach to the protection of personal information, including the acceptance of self-regulatory solutions and technological innovations that empower the user. [152]

Thus, standards must necessarily be flexible while providing a core of rights for individuals. In addition, compliance costs with these standards must be reasonable.

CODES OF PRACTICE

The capacity to create codes of practice was included because different industries have different needs and practices. This option provides flexibility for different data handling practices to be developed based on an industry's particular needs, while still ensuring that privacy is protected. The codes must be at least equivalent to the privacy standards before approval. Thus, these enforceable codes could vary and replace the privacy standards for particular industry sectors.

The idea of rules drafted by industry being enforced by the government is not new to this country. Already, "in some instances, industry-drafted rules are legally enforceable. For example, building codes adopted by local and state governments routinely incorporate technical industry standards by reference -- a violation of the "self-regulatory" code is itself a violation of law."[153] By developing codes of practice under this scheme, "[e]nforcement and adjudication can also be undertaken by industry organizations."[154]

It has been noted that "where rules are either precise or vague, there are likely to be significant costs to industry in complying. . . . [Whereas when] privacy rules are well drafted, the government regulatory system will have net benefits compared to a system without regulation."[155] Thus, industry involvement in drafting codes of practice will

ensure that the rules are neither too precise nor too vague, and lead to rules that at the same time are beneficial to the industry and protect the privacy of individuals.

DISPUTE RESOLUTION MECHANISM

It is important to set a statutory basis for remedy beyond a constitutional violation. Doing so could eliminate much of the risk that currently attaches to information use and disclosure and establish a level playing field for individuals and businesses.[156] Therefore, while the legislation is flexible enough to allow industry to resolve disputes, it also gives the monitoring agency the authority to review and adjudicate these complaints, and to initiate investigations as an alternative to judicial remedies.[157]

A non-judicial remedy would allow a plaintiff adequate compensation for real injuries rather than have an award swallowed up by legal bills. This would allow violations that cause injury to be resolved in a forum that is less expensive. Businesses would also benefit from this arrangement by having clear guidelines for information practices, a well-defined process for dealing with individual grievances, and an agency which understands its information practices.[158]

ESTABLISH INDEPENDENT AGENCY

To bring consistency and appropriate flexibility to the statutory scheme, and to reduce uncertainty and risk, the OIP recommends that an independent agency be established.[159] Such a monitoring agency should be given the authority to develop, with the assistance of industry expertise and members of the public, and pursuant to the principles of information practice, codes of practice for each industry.[160] This would allow the standards to be implemented in a specific manner tailored to each industry and yet provide a meaningful enforcement mechanism for individuals.[161] The monitoring agency would work actively, using audits and educational tools, with industry to ensure that the standards are put into place in the most effective manner.

The flexible role of the oversight authority is crucial to this proposal because the monitoring method utilized will directly affect the viability of the system. For example, a monitoring mechanism such as those in place in certain European countries, that requires the private sector to report every exchange of information to the oversight authority -- this appears to be an excessive burden to both the private and public sectors.[162] On the other hand, the flexibility of the Asia-Pacific model, which includes developing industry standards, educating the public concerning their rights and adjudicating disputes between individuals and private parties is more consistent with the American philosophy of government's role.[163]

ENDNOTES

[1] *See* THOMAS L. FRIEDMAN, THE LEXUS AND THE OLIVE TREE (1999).

[2] Andrew Gomes, *Ensuring E-Consumer Confidence, Internet Companies Scramble for Credibility,* HONOLULU ADVERTISER , October 11, 1999, at B6. *See also* comments of December 3, 1999 from Dr. Alexander Dix, LL.M., Commissioner for Data Protection and Access to Information, Brandenburg, Germany to the Office of Information Practices. Commissioner Dix wrote that he was convinced that government regulation of good consumer privacy practices will not only have a significant positive impact but is in fact the necessary precondition for e-commerce to be attractive to consumers. Without the building of trust in security and privacy protection through effective regulation and monitoring e-commerce will probably not play a significant role in supporting a state's economic growth. *Id.*

[3] Bruce Slane, *Privacy Protection: A Key to electronic Commerce*, paper presented to the June 27, 1999 APEC Electronic Commerce Steering Group Meeting in Auckland, New Zealand.

[4] Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 498 (1995); Robert M. Gellman, *Can Privacy Be Regulated Effectively On A National Level? Thoughts On The Possible Need For International Privacy Rules*, 41 VILL. L. REV. 129, 130-131 (1996).

[5] Jim Donaldson, *You Can Keep Your Privacy, But It Will Take Some Doing*, GANNETT NEWS SERVICE, March 6, 1996; Jay Greene, *They're Selling Your Secrets*, ORANGE COUNTY REGISTER, April 21, 1996, at A1.

[6] INFORMATION POLICY COMM., NAT'L INFORMATION INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE 44 (1997) [hereinafter OPTIONS PAPER].

[7] Mary Zahn & Eldon Knoche, *Electronic Footprints Yours are a lot easier to track than you may think*, MILWAUKEE SENTINEL, Jan. 16, 1995, at 1A. Examples include lists of credit card purchases, purchases made with discount cards at grocery stores, 800 numbers called, magazine subscriptions, driver's license records, real estate records, medical information, and Internet sites visited. All of this information can be combined to create thorough profiles of consumers preferences and needs. *Id.*

[8] Outside of the federal government and to some extent state governments, the collection, use, sale and dissemination of personal information is unregulated

[9] *See* Greene, *supra* note 5, reporting consumers willingly accept the trade-off of releasing information as long as they receive something in return.

[10] Larry Tye, *List-Makers Draw A Bead On Many*, BOSTON GLOBE, Sept.6, 1993.

[11] *Id.*

[12] OPTIONS PAPER, *supra* note 6, at 6-7, examples include disclosing financial information to obtain a mortgage or medical information to get insurance coverage. *Id. See also* Tye, *supra* note 10, quoting Janlori Goldman [head of ACLU Privacy Technology Project] "You have no choice in the world but to give out information about yourself if you want to participate in even the most minimal level of society." *Id.*

[13] Several egregious examples demonstrate this potential; a woman unknowingly made accommodations at a location which rents its mailing list and describes its clientele as primarily " a sophisticated and wealthy lesbian market." The woman is flooded with homosexual related junk mail. *Id.* A couple suffers the miscarriage of their baby but is bombarded daily with junk mail for infant related products. Greene, *supra* note 5. A banker cross-references a list of loan customers with a list of cancer patients and called in the loans of the matches. Jennifer A. Katze, *Who's seeing your files?*, BALTIMORE SUN, July 14, 1996, at E1.

[14] OECD RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, Sept. 23, 1980 [hereinafter OECD GUIDELINES]. The Guidelines define "personal data" as any information relating to an identified or identifiable individual (data subject), and establish eight basic principles relating to personal data: 1) Collection limitation 2) Data quality; 3) Purpose specification; 4) Use limitation; 5) Security Safeguards; 6) Openness; 7) Individual participation; and 8) Accountability. *Id.* at 10-11.

[15] *Id.* at 5.

[16] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 ON THE PROTECTION INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (1995) [hereinafter EU DIRECTIVE]. 1995 O.J.(L 281) 23/11/1995 p.003.

[17] Alliance for Global Business, A GLOBAL ACTION PLAN FOR ELECTRONIC COMMERCE, 2ND EDITION, OCTOBER 1999, AT WWW.GIIC.ORG/FOCUS/ECOMMERCE/AGBEPLAN.

[18] PRIVACY TIMES, July 6, 1999, p. 3. The Minnesota Attorney General had filed a lawsuit against U.S. Bancorp, which had given, in exchange for a commission, customer names and credit card numbers to telemarketers. The telemarketers offered a 30 day "free" trial for travel clubs or dental services, and unbeknownst to the customers their credit cards were billed. The suit was settled on June 30, 1999, with U.S. Bancorp agreeing to, among other things, stop sharing data with third parties for marketing non-financial products and services, pay the state $500,000, and contribute $2.5 million to various charities. *Id.*

[19] PRIVACY TIMES, July 6, 1999, p.2. The February 1998 *Washington Post* reported that CVS Pharmacy and Giant Pharmacy were providing customer data to a Massachusetts database company for the purpose of convincing customers to try new drugs, or refill current prescriptions. Some of the mailings were paid for by Glaxo Wellcome, Merck, Hoffman-LaRouche, and Warner-Lambert. The reports caused such an uproar that both pharmacies ended the programs within 48 hours. *Id.*

[20] The complete text of the DMA's Privacy promise can be found at <www.the-dma.org>.

[21] The complete text of the IRSG principles is available at <www.irsg.org>.

[22] Interview with Graham Greenleaf, Associate Professor of Law, University of New South Wales, Sydney, Australia.

[23] Interview with Bruce Phillips, Privacy Commissioner of Canada, Ottawa, Ontario, Canada.

[24] Dr. Alan Westin and Louis Harris and Associates, Inc., *E-Commerce & Privacy: What Net Users Want*, xii (June 1998).

[25] *Id.* at xi.

[26] *Id.*

[27] PRIVACY TIMES, September 8, 1999, p.9.

[28] *Id.* at 10.

[29] *Id.*

[30] *See* FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES xiv (1989) [hereinafter FLAHERTY]. Flaherty comments that electronic surveillance is the primary concern of data protection and offers the following explanation, "References to 'surveillance' in this volume primarily denote supervision, observation, or oversight of individual behavior through the use of personal data rather than through such mediums as a camera or a private detective." *Id.*

[31] COLIN J. BENNETT, REGULATING PRIVACY 19 (1992).

[32] *Id.* Bennett defines computer profile as, "the derivation of classes of individuals most likely to engage in activities of interest to the agency in question." *Id.*

[33] *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 153 (1996) [hereinafter DATA PRIVACY LAW]. Schwartz and Reidenberg describe how lists of people with various diseases are available for purchase from direct marketing companies, how employers use medical information to shift the health care costs to employees and against worker's compensation claims, and how insurers use medical information to assess insurance coverage. *Id.*

[34] *Id.* at 261. The authors note that, "the movement of personal and non-personal data around the world is both a critical element of financial services and a key financial services product." *Id.*

[35] Mary Zahn & Eldon Knoche, *Electronic Footprints Yours Are A Lot Easier To Track Than You May Think*, MILWAUKEE SENTINEL, Jan. 16, 1995, at 1A. Other examples include lists of 800 numbers called, magazine subscriptions, driver's license records, real estate records, and Internet sites visited. All of this information can be combined to create thorough profiles of consumers preferences and needs. *Id.*

[36] Discussion with Ted Hotham of The Polk Company.

[37] JAMES MICHAEL, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL AND COMPARATIVE STUDY, WITH SPECIAL REFERENCE TO DEVELOPMENTS IN INFORMATION TECHNOLOGY 8 (1994) [hereinafter MICHAEL].

[38] Adam L. Penenberg, *The End of Privacy,* FORBES, November 29, 1999, at 183.

[39] *Id.*

[40] *See* Michael Stroh, *An Eye on Privacy: The Internet allows Commercial Big Brother to Know More About You than You Want Him To*, HONOLULU ADVERTISER, October 22, 1999, at D1.

[41] *Id.*

[42] Penenberg, *supra* note 38, at 183. One such company, Docusearch will provide a client with your unlisted telephone number or Social Security number for $49, your bank balances for $45, driving record for $35, cell phone number for $85, or provide a list of stocks, bonds, and securities you own for $209. *Id.* at 184.

[43] *Id.* at 183-186

[44] Phillip Morris, *Document Search Sites put your Private Life on the Internet,* CLEVELAND PLAIN DEALER, reprinted in THE HONOLULU STAR-BULLETIN, December 11, 1999 at B4.

[45] *Id.*

[46] *Id.*

[47] Wired News Report, *RealNetworks in Real Trouble,* WIRED NEWS SERVICE, November 10, 1999.

[48] DATA PRIVACY LAW §2-2(a) , *supra* note 33, at 13.

[49] *Id.* §2-2(b), at 15.

[50] *Id.* §2-2(c), at 16.

[51] Throughout this paper, the authors will refer to these four elements as the Schwartz and Reidenberg model.

[52] *See* Gellman, *supra* note 4, at 135.

[53] *See* FLAHERTY, *supra* note 30, at 305-306.

[54] 5 U.S.C. §522a (1994).

[55] FLAHERTY, *supra* note 30, at 306.

[56] *See* DATA PRIVACY LAW, *supra* note 33, at 93.

[57] *See generally* DATA PRIVACY LAW §5-2(a) , *supra* note 33.

[58] 5 USC §552a(b)(3).

[59] DATA PRIVACY LAW §5-2(a) , *supra* note 33, at 98-100.(discussing that the only remedy courts can fashion is an injunction for the agency to desist the particular action for a particular individual therefore judicial authority is severely limited). *See also Id.*, §5-5(a) at 115.

[60] FLAHERTY, *supra* note 30, at 341.

[61] DATA PRIVACY LAW §2-2(c), *supra* note 33, at 16.

[62] DATA PRIVACY LAW §5-4, *supra* note 33, at 112. (The Privacy Act prohibits the collection of information relating to the exercise of rights guaranteed by the First Amendment (5 U.S.C. §552a(e)(7)), however, such data may be gathered if it is within the scope of authorized law enforcement activity. All agencies can be considered to involve law enforcement creating an exception which leaves sensitive information vulnerable to disclosure). *Id.*

[63] *See* COLIN J. BENNETT, REGULATING PRIVACY 176-77.

[64] *See* Mary Zahn & Eldon Knoche, *Electronic Footprints Yours are a lot easier to track than you may think*, MILWAUKEE SENTINEL, Jan. 16, 1995 at 1A (reporting that the F.B.I. inquired about the services of direct marketing company Metromail; noting the Selective Service case of buying the names of customers of an ice cream parlor registered for free dessert on their birthdays in order to remind males to

register for the draft; the I.R.S. rented commercial mailing lists to try and catch tax cheats) *Id.*; *See also* Thomas B. Rosenstiel, *Someone May Be Watching*, LOS ANGELES TIMES, May 18, 1994 at A1 (noting that a General Accounting Office report in 1990 showed 910 federal databases many of them shared with corporations and commercial databases).

[65] The limited success of the Privacy Act of 1974 comes in conjunction with the Freedom of Information Act (5 U.S.C. §552); *See* DATA PRIVACY LAW §5-3(b), *supra* note 33, at 108-111.

[66] *See* Reidenberg, *supra* note 4 at 500-501, (author noting that this practice has become entrenched in American politics and is driven by the desire to "minimize restrictions on information flows" and the desire to "disperse standards setting") *Id.*

[67] The most often cited example being the result under current federal legislation that one's video rental records are better protected than the confidentiality of one's medical records, *See* G. Bruce Knecht, *Privacy: A New Casualty in Legal Battles: Your Privacy*, WALL STREET JOURNAL, April 11, 1995 at B1, (quoting Robert Gellman, "If someone had tried to get Bork's medical records, we'd have a law for medical records.")*Id.*

[68] 15 U.S.C. §1681. Credit information is a cornerstone of American business, and credit reporting agencies process every transaction involving credit covering about 170 million Americans, DATA PRIVACY LAW §11-2, *supra* note 33, at 286; *See also* OPTIONS PAPER, *supra* note 6, at 38.

[69] DATA PRIVACY LAW §11-2, *supra* note 33, at 289.

[70] The legal mechanism may be ineffective as it is difficult to remove one's name from a list.

[71] Cheryl B. Preston, *Honor Among Bankers: Ethics in the Exchange of Commercial Credit Information and Protection of Customer Interests*, 40 U. KAN. L. REV. 943, 995 (1992).

[72]Omnibus Consolidated Appropriations Act, Pub. L. No. 104-208, tit.2, 110 Stat. 3009 (1996), significantly imposing upon creditors obligations relating to the accuracy of information furnished to credit reporting agencies, OPTIONS PAPER, *supra* note 6, at 41.

[73] Although the Act may bring all these services "under one roof" in the interest of "consumer convenience," it also provides the opportunity for these previously separate companies to become one company or "affiliates." The privacy protections provided by the Act do not apply to the disclosure of information between these affiliated companies.

[74] *Plenty of Thorny Issues to Be Ironed Out in Privacy Rules*, AMERICAN BANKER, December 7, 1999.

[75] 18 U.S.C. § 2710.

[76] *See* OPTIONS PAPER, *supra* note 6, at 42.

[77] *See* Gellman, *supra* note 4, at 146. (discussing that similar activities such as library records or magazine subscriptions are not covered by any legislation and that the current laws do not cover direct broadcast satellite or wireless communications). *Id.*

[78] 12 U.S.C. 1304 et seq.

[79] Exceptions include the release of records as incident to perfection of security interest, proving a claim in bankruptcy, collecting a debt, or processing an application with regard to a Government loan, and

loan guarantees. The RFPA establishes notice requirements and procedural protections for those to whom the financial records pertain. *Id.*

[80]15 U.S.C. 41 et seq.

[81] *See, e.g.*, 15 U.S. C. 1818 et seq., the Federal Deposit Insurance Act.

[82] 15 USC 6501 et seq.

[83] *See* JANLORI GOLDMAN & DEIRDRE MULLIGAN, CENTER FOR DEMOCRACY & TECHNOLOGY, PRIVACY AND HEALTH SYSTEMS: A GUIDE TO PROTECTING PATIENT CONFIDENTIALITY 3 (1996), (citing several examples including a Boston-based HMO admitting to recording detailed notes from psychotherapy sessions on a computer accessible by all clinical employees, and a New York politician had hospital records of her attempted suicide and depression publicly disclosed). *Id.*

[84] *But see* Jim Donaldson, *You Can Keep Your Privacy, But It Will Take Some Doing*, GANNETT NEWS SERVICE, March 6, 1996.

[85] *See* DATA PRIVACY LAW §2-1(b), *supra* note 33, at 10-11.

[86] *See* Bruce D. Goldstein, *Confidentiality and Dissemination of Personal Information: An Examination of State Laws Governing Data Protection*, 41 EMORY L.J. 1185.

[87] DATA PRIVACY LAW ch. 6, *supra* note 33, at 129-151.

[88] DATA PRIVACY LAW, *supra* note 33, at 132. (The authors indicate that the states with the strongest levels of data protection, i.e. California, have a constitutional basis for the right of privacy. In Hawai`i, *See* HI. CONST. art 1, §6). *Id.*

[89] DATA PRIVACY LAW §6-1, *supra* note 33, at 135. The corresponding Hawai`i statute is the Uniform Information Practices Act (Modified) HAW.REV.STAT. §92F (1988).

[90] DATA PRIVACY LAW §6-5, *supra* note 33, at 144. The oversight agency in Hawai`i is the Office of Information Practices, established by HAW. REV. STAT. §92F-41.

[91] *See generally*, ANNE F. LEE, THE HAWAII STATE CONSTITUTION A REFERENCE GUIDE 47 (1993) [hereinafter LEE].

[92] HI. CONST. art. 1 §6.

[93] LEE, *supra* note 93, at 46; "Informational privacy" is described as the ability of a person to control the privacy of information about himself, privacy in the "personal autonomy" sense means the right to control certain highly personal and intimate affairs of his own life. The focus of this discussion will be privacy in the informational sense, *See* H.R. STAND. COMM. REP. No. 69, 14th Leg., Reg. Sess. (1988), *reprinted in* 1978 Constitutional Convention Documents 674.

[94] H.R. STAND. COMM. REP. No. 69, 14th Leg., Reg. Sess. (1988).

[95] *Id.* at 675.

[96] *Id.*

[97] Committee of the Whole Report No. 15, *reprinted in* 1978 Constitutional Convention Documents at 1024.

[98] State Of Hawai`i Organization Of Police Officers (SHOPO) v. Society Of Professional Journalists - University Of Hawai`i Chapter, 83 Haw. 378, 397, 927 P.2d 386, 405 (1996). The court quoted both the Standing Committee Report No. 69, *supra* note 94, and the Committee of the Whole Report No. 15, *supra* note 97. Specifically, the court quoted that, "article I, section 6 'relates to privacy in the informational and personal autonomy sense', and also that the provision was applicable to 'private parties.'" *SHOPO*, 378 Haw. at 397, 927 P.2d at 405.

[99] Painting Industry of Hawaii Market Recovery Fund v. Alm, 69 Haw. 449, 453, 746 P.2d 79, 81-82 (1987). The court was interpreting the scope of the constitutional right as defined by HAW.REV.STAT. §92E which was repealed upon adoption of §92F, the current information practices statute.

[100] Stand. Comm. Rep. No. 69, 14th Leg., Reg. Sess. (1987) at 675.

[101] HI CONST art. I, §6.

[102] HAW. REV. STAT. §92F, L. 1988, c.262; HAW. REV. STAT. §92F, Part II, §§11-19; HAW. REV. STAT. §92F, Part III, §§21-28.

[103] HAW. REV. STAT. §92F-2(5).

[104] *See* DATA PRIVACY LAW §5-3(b) , *supra* note 33 at 108-109. The principles embodied within this element consist of collection of personal information for specific purposes, limited to only those uses compatible with the purpose of its collection, collection of only relevant information, limits on duration of storage, subject access to information, and adequate safeguards to ensure data integrity. *See also* §2-2(a), at 13.

[105] HAW. REV. STAT. §92F-2. The OIP has proposed rules that cover the collection of information by government. These rules remain in administrative review. *See also* Report of the Governor's Committee on Public Records and Privacy vol. 1 p. 64.

[106] HAW. REV. STAT. §92F-19.

[107] HAW. REV. STAT. §92F-21; HAW. REV. STAT. §92F-22 lists instances where disclosure is not required. These exceptions involve; records pertaining to the criminal process, beginning with criminal investigation up through release from supervision; disclosure of a confidential source; testing or examination materials which would compromise the testing or examination; investigative reports of an upcoming, ongoing or pending civil or criminal action; required by law to be withheld. *Id.*

[108] HAW. REV. STAT. §92F-24; the agency must respond to any request to correct within 20 days of receipt. *Id.*

[109] The history of art. I, §6 of the Hawai`i Constitution also indicates that this right of access should be encompassed within the right to privacy. If the intent of the Standing Committee is to be correctly understood that the right of privacy extends to private parties, then this right of access should also be guaranteed outside of the state government. *See* STAND. COMM. REP. No. 69, 14th Leg., Reg. Sess. (1987).

[110] HAW. REV. STAT. §92F-18, this monitoring role helps the individual discover how his records are being used and who is seeing them.

[111] HAW. REV. STAT. §92F-13(1).

[112] *See* DATA PRIVACY LAW §6-5, *supra* note 33, at 145-148. (The authors describe that even states having data protection legislation, oversight is the exception. California and Wisconsin are two examples of states which saw their oversight agencies cut for budgetary reasons. *Id.* at 146. This demonstrates what a unique position Hawai`i holds among American jurisdictions. (This text only notes two oversight agencies which remain active: New York's Committee for Open Government, N.Y. PUB. OFF. LAW §§84-98; Minnesota's Commissioner of the Department of Administration, MINN. STAT. §§13.06 et seq.).

[113] HAW. REV. STAT. §92F-42.

[114] DATA PRIVACY LAW §2-2, *supra* note 33, at 12.

[115] *See generally* DATA PRIVACY LAW §6-5, *supra* note 33. This breakdown of responsibilities is the result of analyzing the functions stressed by the authors in the text.

[116] HAW. REV. STAT. §92F-42(1),42(3),42(8).

[117] HAW. REV. STAT. §92F-42(4),42(5).

[118] HAW. REV. STAT. §93F-42(12)-42(15) and Act 87 (1999).

[119] HAW. REV. STAT. §92F-21; HAW. REV. STAT. §92F-24.

[120] HAW. REV. STAT. §92F-27; HAW. REV. STAT. §92F-27.5. An individual does not have to go through OIP before going to circuit court, but the individual must exhaust his administrative remedies under 92F-23, 92F-24, and 92F-25, before bringing suit.

[121] *See generally* HAW. REV. STAT. §92F-42.

[122] HAW. REV. STAT. §92F-28; HAW. REV. STAT. 92F-27(c).

[123] *See* DATA PRIVACY LAW §6-2, *supra* note 33, at 132 (authors stating that California has the most comprehensive approach to data protection, however, the authors subsequently note that California has no oversight agency). *Id.*

[124] DATA PRIVACY LAW §2-2, *supra* note 33, at 12.

[125] ECONOMIC IMPACT: U. S. AND DIRECT INTERACTIVE MARKETING TODAY, 1999 FORECAST 12 (5th edition).

[126] *Id.* at 11.

[127] The official position of the Clinton administration on Internet privacy is that the market should lead through self-regulatory efforts. However, if self-regulatory efforts are not successful, the Administration has stated that it will reconsider its position. Peter Swire, *United States: Privacy Update*, remarks given at the Second Asia Pacific Forum on Privacy and Personal Data Protection, September 12, 1999.

[128] Peter Swire, Markets, Self-Regulation and Government Enforcement in the Protection of Personal Information (1996), <www.osu/units/law/swire1/psnita6.htm.>.

[129] *Id.*

[130] Reidenberg, *supra* note 4, at 508 (1995).

[131] *See* Declan McCullagh, *Is TRUSTe Trustworthy?*, WIRED NEWS SERVICE, November 5, 1999.

[132] *Unfair Trade Practices Complaint Filed Against Truste/AOL*, PRIVACY.NET, <http://www.privacy.net/truste.asp>.

[133] *Id.*

[134] *Id.*

[135] *'Secure Assure' Looks to Challenge TRUSTe as Leading Privacy Seal*, PRIVACY TIMES, November 23, 1999, at 5.

[136] For example, in New Zealand, an individual may complain to the Privacy Commissioner for any violation of the Privacy Principles by any person, corporate or otherwise, public sector or private sector. *See* N.Z. Privacy Act, Art. 2, 67.

[137] Alliance for Global Business, A GLOBAL ACTION PLAN FOR ELECTRONIC COMMERCE, 2ND EDITION, OCTOBER 1999, *supra* at n.17. (With a freely functioning global electronic marketplace, increasingly sophisticated, user friendly tools and business practices for empowerment of consumers have been and continue to be developed and implemented.) *Id* at 22.

[138] *Id.*

[139] Swire, *supra* note 128.

[140] The Alliance for Global Business has stated "Business uses model contracts and internal control procedures to satisfy requirements of legislation restricting export of data to third countries that do not provide a level of protection or sufficient by the source country. The use of model contracts provides a flexible, market-based solution for meeting differing data protection standards in the conduct of global business." Alliance for Global Business, A GLOBAL ACTION PLAN FOR ELECTRONIC COMMERCE, 2ND EDITION, OCTOBER 1999, *supra* note 17, at 20.

[141] Alliance for Global Business, A GLOBAL ACTION PLAN FOR ELECTRONIC COMMERCE, 2ND EDITION, OCTOBER 1999, *supra* note 17, at 20.

[142] H.B. 1232 and S.B. 991.

[143] *SHOPO* 83 Hawai`i 397, 927 P.2d 405.

[144] *See generally* Reidenberg, *supra* note 4.

[145] *See* Thomas B. Rosenstiel, *Someone May Be Watching*, LOS ANGELES TIMES May 18, 1994 at A1, reporting that Kroll Associates has access to over 700 online databases making them second only to the federal government; *see also* Reidenberg, *supra* note 4, AT 532 & n. 192. (Reidenberg notes that several key private sectors have a significant impact on the daily lives of citizens and that the treatment of information in these sectors could lead to "improper coercion." These sectors include among others employment, health care, financial services and education). *Id.*

[146] Swire, *supra* note 128.

[147] HI CONST. Art. I, §6. The right to privacy *shall not be infringed upon* absent a compelling state interest; see also DATA PRIVACY LAW §4-2, *supra* note 33, at 35.

[148] DATA PRIVACY LAW §2-2(a), *supra* note 33, at 13.

[149] Alliance for Global Business, A GLOBAL ACTION PLAN FOR ELECTRONIC COMMERCE, 2ND EDITION, OCTOBER 1999, *supra* note 17.

[150] Similar standards were proposed to the Hawaii Legislature in H.B. 1232 and S.B. 991 in 1999.

[151] *See* James R. Maxeiner, *Business Information and "Personal Data": Some Common-Law Observations About the EU Draft Data Protection Directive*, 80 IOWA L. REV. 619, 621-622, (1995).

[152] Alliance for Global Business, A GLOBAL ACTION PLAN FOR ELECTRONIC COMMERCE, 2ND EDITION, OCTOBER 1999, at 20 *supra* note 17.

[153] Swire, *supra* note 128.

[154] *Id.*

[155] *Id.*

[156] See *SHOPO* 83 Haw. at 398, 927 P.2d at 406 the Hawai`i Supreme Court indicates that, in the absence of statutory standards, violations of informational privacy are to be considered in terms of tort liability for invasion of privacy.

[157] The Alliance for Global Business proposed to governments, in its paper entitled A GLOBAL ACTION PLAN FOR ELECTRONIC COMMERCE, 2ND EDITION, OCTOBER 1999, stated that out-of-court dispute settlement procedures for consumers should be encouraged while maintaining court proceedings as the ultimate solution in case of conflicts, *supra* at note 17, at 22. Such a mechanism could also be modeled after HAW. REV. STAT. §92F-42 and would provide individuals a remedy for those minor breaches which would ordinarily be cost-prohibitive to take to court.

[158] *See* Joel R. Reidenberg & Françoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, WAKE FOREST L. REV. 105, 108-9 (1995)(authors noting that while individuals certainly have an interest in the treatment of personal information, businesses also benefit by having a structure in place to ensure the quality and integrity of the information upon which they must rely). *Id.*

[159] This provision was not in H.B. 1232 or S.B. 991. Whether the legislature should create a new agency or utilize an existing office is a policy decision. Given the State's current fiscal constraints, and the fact that the OIP already exists as an independent agency monitoring the information practices of the government sector, the OIP recommends that the legislature have the OIP administer any legislation dealing with the privacy of personal information in the private sector rather than creating a new office.

[160] It has been the New Zealand approach to work with a specific sector to develop the nature of acceptable information practices for the entire industry; additionally HAW. REV. STAT. §91 requires that if an agency intends to promulgate rules it must first hold a public hearing. This would provide the forum for open discussion of what standards would be enacted above the broad principles found in the statute.

[161] *See generally*, Reidenberg, *supra* note 4.

[162] Neither New Zealand nor Quebec require the registration of private sector databases.

[163] *See* OPTIONS PAPER, *supra* note 6, at 52.