The 14th Congressional District's
Student Advisory Board

Privacy as it Pertains to Civil Liberties

2003 Annual Report

Saturday, May 17, 2003

PRIVACY AS IT PERTAINS TO CIVIL LIBERTIES

Introduction

Nikhil Warrior, Chairperson

We, the members of the Student Advisory Board hoped to take the wonderful opportunity that had been given to us, and use it to make our voices heard on issues that had real significance. We are all very grateful to Rep. Anna Eshoo for giving us this important chance, and we all give her our most sincere thanks.

When the Student Advisory Board first convened we were confronted by a broad array of possible topics, from things such as foreign policy initiatives to women's issues to cows. There were a few commonalities among people's interests. The members were still moved by the events of September 11th, and there was a palpable desire to do something that would be connected to it. The other factor was that we wanted to deal with a really substantive issue that affected us, all of us, on a personal level. We found the crossover between these two directives in privacy. We felt we could examine both issues of individual significance, such as consumer privacy, and at the same time tackle what we see as a dangerous erosion of civil liberties in our country.

Thus we tried to split up the report between generic privacy and civil liberties oriented privacy. In our report we cover: consumer privacy, Internet privacy, biometrics, medical/ public records, surveillance, The Patriot Act, and the registration of immigrants. Each one of the topics represents an important facet of the greater field of privacy.

Student Survey

Julia Duncan, Zayra Diaz, Liesl Pollock, Nick Deming, Margaret Ren, Grant Toeppen, Lauren Habig

Background

During this year the Survey Committee of Congresswoman Anna Eshoo's Student Advisory Board has researched and determined what the average high school student knows about their privacy rights and the amount of personal information that is accessible over the internet. It is surprisingly easy to find personal information such as social security numbers, addresses and phone numbers of citizens in large databases full of crucial personal information. Critical information even appeared for those people who have specifically requested not to be listed in such databases.

Through research, which included surveying five high schools in the Fourteenth Congressional District, we have found that over all, students seem to be ill-informed about their right to privacy or the issues that surround this complex topic.

As part of our research, the Survey Committee distributed surveys to five high schools in the 14th Congressional District. A total of 400 surveys were circulated. The results yielded enough information to conclude that high school students in the 14th Congressional District are not well informed about their rights to privacy and the issues that surround privacy.

Our survey yielded some interesting results. For example, of the students surveyed over 54% believe that biometrics, including finger printing, face screening and DNA profiling by the government is not an invasion of personal privacy. A majority of students surveyed also said that they would be comfortable knowing that their DNA was in a government data base.

Throughout the research it was clearly evident that there are various websites that disclose personal information about the general public. Websites such as *ancestry.com* can be useful for finding information about relatives, but they also have the capacity to give out critical information such as social security numbers to anyone who logs onto the site. Because all the people listed on this site have been deceased for at least one year, it makes it extremely effortless for others to steal their identities. In addition many people are not aware that their right to privacy has been violated.

Analysis

It is upsetting that this private information can be accessed easily, quickly and for free. It used to be that someone's social security number was private and was something that was not given out to others, but with the use of technology, these essential numbers have become the whole world's business.

It is important to keep private information off the internet if people do not wish their information to be made available. At this point in time, the government has not taken sufficient steps towards ensuring peoples' privacy rights, as can be seen by the excess of personal information circulating on the internet. The government must elevate its response to the very pertinent threat of violations of privacy rights, specifically by monitoring the amount of important personal information that can be on the internet without permission from the owner of said personal information. It is also the government's responsibility to protect the citizens' privacy and to prevent individuals' personal information from circulating through the internet without their authorization, or

at the very least, their knowledge. The government might consider putting restrictions on large databases that contain personal information in order to make sure that its citizens' information is protected from being available to the general public. Companies that post private information on the internet need to be regulated so that they act responsibly in providing sensitive personal information to persons logging onto their site. Particularly important is the prevention of identity theft, especially when information from those who are deceased can be easily accessed by anyone in the world.

In addition to being the government's responsibility to protect its citizens, it is also each citizen's responsibility to inform him or herself about issues surrounding privacy and to be mindful of giving out personal information. Each individual needs to be aware of the potential risks involved when giving personal information to unverified sources, such as websites and scam artists who prey on those who are ill informed. Individuals should perform a search on themselves on the internet to determine whether any of their personal information is available to other internet users.

We feel that education is one thing we need to focus on in order to ensure that all people have a right to personal privacy. On our survey we found that many students neglected to answer question number 9 which asks, "Do you believe that the Patriot Act is beneficial?". Approximately one-third of the students did not answer this question. We may be able to conclude from this lack of response, that this question was not answered because of the lack of knowledge people had about the Patriot Act.

As society advances technologically, especially with the advent of the internet, the confidentiality of citizens' personal information is further put into jeopardy. While it is still a subject of debate whether or not the Constitution of the United States provides its citizens with an explicit right to privacy, Supreme Court cases, such as Roe v. Wade, over the past decades have ruled that citizens of the United States do have some rights where privacy is concerned. However, the surveys distributed by members of Congresswoman Anna Eshoo's Student Advisory Board overwhelmingly demonstrated that high school students are not informed as to the issues surrounding their privacy and personal information. When confronted with a problem, the first step to a solution is familiarization with all facts of the issue. People, specifically high school students, must be taught more about their rights to privacy and protecting their personal information. In addition, they should be more mindful of how they disclose their personal information, and to whom. The government, too, has a role to play: legislation along the lines of the Cyber Security Research and Development Act would be a step in the right direction, as well as further measures to monitor and to restrict the unauthorized distribution of personal information on the internet. Privacy of personal information, while ill defined under United States law, is an issue that affects citizens on a frequent basis. They must become better informed as to their rights, and their rights must be further protected.

The Student Advisory Board feels that the government must put restrictions on the amount of personal information that can be given to someone about another person. It is imperative that we remove crucial information such as social security numbers from the internet to protect the privacy and safety of all citizens.

Consumer Privacy

Preeti Piplani, Elizabeth Ashton, Derek Fletcher, Kalpana Sundaram

Topic: Telemarketing regulations

Background Information

On December 18, 2002, the Federal Trade Commission (FTC) amended the Telemarketing Sales Rule (TSR) and created the "Do Not Call Registry." The Do Not Call Registry is designed to help stop telemarketers from soliciting households. Any individual can sign up for the FTC's registry to stop receiving telemarketing calls after 9:00 p.m. and before 8:00 a.m. A roster with the names and phone numbers of the individuals on the Do Not Call Registry will be distributed to all professional telemarketing companies on September 1, 2003, after the TSR is implemented on July 1, 2003. Telemarketers who do not comply with the TSR face stiff fines of $11,000 per telephone call made to individuals on the list. By creating and implementing the TSR, the Federal Trade Commission aims to stop unwanted telemarketing calls which are an abridgement of consumer privacy rights.

Flaws with the TSR

While the Do Not Call Registry is a step toward protecting consumer privacy, the amended TSR still contains several loopholes. This new legislation claims only to "stop most but not all telemarketing calls." This loose terminology provides for many exemptions and subjective interpretations of the TSR. For example, the TSR allows for the exemption of telemarketing calls from banks, telephone companies, airlines, surveys, charities, political campaigns and fundraisers. These organizations are only limited to the extent of state regulation by each respective state. The TSR does not protect consumers from telemarketing calls during the hours of 8:00 a.m. to 9:00 p.m. when most unwanted calls are made. When reporting violations of the TSR, consumers are often unable to prove that they were illegally contacted by a telemarketer. If a consumer were to report a violation, he would need to report:

-the consumer's name, address, and daytime phone number
-the action the consumer is requesting against the telemarketer
-the date the consumer was added to the Do Not Call Registry
-the name of the individual the consumer spoke with
-the organization name, address and telephone number of the telemarketer
-the date and time the consumer was contacted by the telemarketer

This information is often difficult to obtain as many telemarketers simply hang up after the consumer begins to question the telemarketer.

Recommendations and Suggestions

The TSR is a launch pad for future legislation and regulations against unwanted telemarketing phone calls. Past legislation like the 1991 Telephone Consumer Protection Act protects consumers by allowing them to sue telemarketers for up to $500. Yet stricter filters are needed in order to help weed out telemarketers. New legislation with stricter regulations against telemarketers is currently in the House of Representatives and is crucial to further protection of consumer privacy. H.R. 1636 introduced to the House and

H.R. 1330 both include immediate legislation to increase consumer privacy. H.R. 1330 would specifically restrict telemarketing calls during the hours of 5:00 p.m. and 7:00 p.m. Since these bills are both in the House Energy and Commerce Committee, Representative Eshoo could directly advocate stricter telemarketing regulations. Future legislation must be introduced to help create a more efficient manner of recording illegal telemarketing calls. Additionally, the current information required to report an illegal call is lengthy, difficult to obtain, and almost impossible to document without the aid of a recording device or caller ID. While Congress is gradually working to improve violations of telemarketing calls, our group believes that Representative Eshoo is a necessary catalyst in this process and we hope her advocacy will result in further telemarketing regulation.

Internet Privacy

Hilary Englert, Danielle Paya, Mike Yost, Helen Rhee

Background

Internet privacy is an issue concerning our society today. Privacy is a right protected under the Bill of Rights. It states that authority can't search a person without a warrant. However, many people's rights are violated many times a day on the Internet. Many users' private information is shared between companies without consumers' prior knowledge. Many users are tracked and recorded by companies for their financial gain. There are also growing problems of harassment and abuse. Most of all, there are problems of internet fraud and scams, and proliferation of personal information on Internet. This paper will discuss main problems of Internet use.

Unsolicited e-mail is a growing problem faced by many Internet users today. Some states have outlawed unsolicited e-mail. According to the website Internet Attorney, federal judges in Philadelphia have declared that companies do not have the First Amendment right to send unsolicited commercial e-mails to Internet users. However, even under the regulation by law, the problem of unsolicited commercial e-mail has not been completely solved. Unsolicited e-mail is not only irritating but it is financially unfavorable. It costs Internet users and Internet-based companies millions of money. According to the Coalition Against Unsolicited Commercial E-mails group, "Junk e-mail is 'postage due' marketing; it's like a telemarketer calling you collect. The economics of junk e-mail encourages massive abuse and because junk e-mailers can get into the business very cheaply, the volume of junk e-mail is increasing every day."

There are different kinds of junk mail according to the Coalition: Chain letters pyramid schemes (including Multilevel Marketing, or MLM), other "Get Rich Quick" or "Make Money Fast" (MMF) schemes, offers of phone sex lines and ads for pornographic web sites, offers of software for collecting e-mail addresses and sending UCE, offers of bulk e-mailing services for sending UCE, stock offerings for unknown start-up corporations, quack health products and remedies, and illegally pirated software ("Warez"). These e-mails lead to many problems such as fraud, ethics violations, displacement of normal e-mails, and cost-shifting. This costs internet providers more money since unsolicited e-mails slow down the bandwidth rate. Even though there are many products that claim to solve the problems of unsolicited e-mails, there has been no product that has completely solved the problem.

There are also growing problems of defamation. According to Internet Attorney, "Defamation consists of false and unprivileged publication which results in economic damages." These defamation postings include cases of false medical reports, harmful material against the businesses and individuals, and hate messages.

Loss of trade secrets and confidential information, as well as increased hacking, are a growing problem in which confidential and financial information of a company is revealed to public without prior knowledge of the company. This can leave millions of dollar in damages to the company. This not only applies to companies; individuals are also becoming the victims. Some individuals lose their financial information, such as a credit card number, online.

According to Congressional Research Services, in 1998, the online industry created an online privacy alliance to promote industry self regulation. They formed a set of

privacy guidelines that encourage the members to adopt and to abide by. The Better Business Bureau, trustee, and web trust all have established "seals" which display a company's privacy policies. This is called the "opt-in" method which refers to a requirement that a consumer give affirmative consent. However, these methods do not fully guarantee one's privacy. Most consumers do not care or have time to read the complicated jargon of the privacy statement. Therefore, they may give affirmative consent without actually understanding the privacy statement. This poses a threat to consumers who do not understand the danger of signing into a privacy statement without any knowledge. There is also a method call "opt-out" which assumes a consumer's permission unless notified by the consumer. This is another problem. Everyday busy Americans may not have the time to request a privacy statement before they visit the site. It is mostly disregarded by many people.

There are also concerns about online profiling. Online profiling is where companies collect personal data about the consumer's taste and preferences. They track the websites that the consumer visited and form a user preference. They then use this information for targeted advertising. Some companies even sell this personal information. There have been attempts by the Congress to solve this problem. In 107th congress, the Bankruptcy Reform bill would have prevented companies and website operators on bankruptcy from selling or leasing consumer information (from online profiling) to a third party.
These are only a sample of problems posed by Internet use. It is imperative that our government look closely into monitoring and regulating internet community. Furthermore, it is important to protect our privacy.

Availability of Personal Information

Several groups like advertisers, sellers, and identity thieves are after personal information. Advertisers pursue personal information because the better and more accurate information they can compile on a consumer, the more they are loaded with useless hassles, like popup windows on the internet or junk mail in mailboxes. They are after personal information because simple statistics show that if they advertise more, more people are aware of their products and consequently more people buy them. Sellers, however, are a slightly different group in that they have an advantage. The seller already knows that the customer is interested in their product and can sell that interest to others or use it to offer tantalizing sales in the future. This highly targetable sales method increases their revenue tremendously—after all, a repeat customer is invaluable in commerce. The most subversive of those after personal information is the identity thief. This character must act in secret, because as soon as the information is discovered missing, passwords and credit cards are changed, making the old information worthless. Unfortunately, the goods that these thieves steal are unlike material goods, in that it's very difficult to tell if personal information is stolen. Once a thief has this information, surprisingly personal advertisements might appear if the thief sells the information to a vendor or fraudulent credit card charges may appear on the next bank statement.

There are a few easy methods of identity theft that are just as easily prevented, like carelessly posting information, using free software ("freeware"), and using internet "cookies." Naïvely posting personal information when applying for free services online, like a game network or email address, often leads to valuable advertising information. Even if the information is only given with a zip code, it provides demographic

information that leads to more targeted advertising in the area. Another subversive method is freeware, which often times is a carrier for "spyware," a program that installs itself on the computer with the free program and reports whatever it is told to record to a website. Even Norton, the company that makes the well-known antivirus program, was the recent victim of some moderately well-done spyware. The danger of spyware is that the information can be excruciatingly specific, leading to very valuable information. Cookies, on the other hand, are less subversive but just as useful. Cookies are tiny bits of data that websites upload in order to identify a particular computer to their website. While this can lead to very accurate and personable service, which contributes to the motive for a vast majority of major websites using them, this information could also be sold easily for profit.

The consequences of identity theft can range from simple spam mail to targeted advertising or, worst case scenario, illegal credit card charges. Spam is the useless deluge of junk mail that everyone has seen—an advertisement for some obscure product in the mail or flyers almost randomly spread out. Usually this is not a large identity theft problem, but it does pose an annoying hassle for most people. Targeted, or narrow-cast, advertising is the advertising that is directed specifically at consumers, like telling a guitarist about a sale on a new speaker that could be coming in at a store. Narrowcast advertising is highly profitable, as there is a comparatively excellent chance that the consumer will be interested and buy the product. The worst problem that can occur with identity theft is false credit card charges. In these cases, thieves use their pilfered information to apply for credit cards. Since this usually only takes two id's, it is not very difficult to make up a card, then run the charges into the thousands before anyone catches wise. The federal government is particularly interested in this last problem, as the thieves are usually so clandestine that consumers are only liable for about $400 of the fraud—the government picks up the rest.

Preventive Measures

Though the consequences of lost Internet privacy can be devastating, there are ways to prevent the ease of acquiring personal information online and off.

- The most important thing to remember is to not give out personal information unless it is required. Be especially defensive with your social security number. This information is vital to your identity and should be protected and kept private at all costs.
- Try to make as many of your purchases as possible with cash. When you use credit cards, order over the Web, telephone, or in catalogs, or use a supermarket discount card, your name will be linked to your purchases in a marketing database. As long as you use cash, there is no electronic trail to connect back to you.
- It is important to be Internet smart as well: protect yourself from "cookies" on your computer that can be used for "data mining" purposes, keep "clean" e-mail addresses free of links to chat rooms or mailing lists, don't respond to spammers, and be conscious of Web security.

Despite the best efforts of anyone, some form of personal information will always be available for the access of others. What is important is preventing this information

from falling into the hands of the wrong people. By following a few of the previously mentioned suggestions, this risk can be reduced.
We propose:

- A federal ban on unsolicited email, or "spam".
- Restrictions on the ease of selling consumer information between companies.
- Limitations in tracking software put in programs, such as spyware.

In addition we feel that consumers need to be made more aware of the risks they take while giving out information online. Realistically, there will never be a guarantee of 100% privacy, but if the necessary regulation is enacted, and information is more difficult to collect, than the privacy of American citizens cans be more safely assured.

Legislation

The development of the Internet has enabled many positive functions, such as purchasing, business use, education and law enforcement. It connects users to anywhere in the world, and is instant. While there have been many improvements, privacy has become a major issue as consumer information is easily accessible. In 2001 a bill was introduced by Representative Anna Eshoo to protect the privacy of consumers who use the Internet, H.R. 237. Yet this bill, the "Consumer Internet Privacy Enhancement Act" died in the 107th Congress. We think that a bill that protects the Internet user and consumers is needed, and that would set a standard for Internet privacy. Legislation in the 108th Congress is similar to Representative Anna Eshoo's Internet privacy act. The "Online Privacy Protection Act," H.R. 69, would require the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected about individuals not covered by COPPA. H.R. 70, the "Social Security Online Privacy Protection Act" would regulate the use by interactive computer services of social security numbers and other personally identifiable information. Legislation passed in the 107th congress that relates to Internet privacy is the "E-government Act," which sets requirements on government agencies in how they ensure the privacy of personal information in government information systems. The "21st Century Department of Justice Authorization Act" requires the Justice Department to notify Congress about its use of Carnivore or Internet monitoring systems similar to Carnivore. Finally, the "USA Patriot Act" expands the ability for the government to monitor Internet activities. All the legislation passed helps protect both the country and individual citizens.

Genetic Privacy

Daniel Wenger and Esen Boyacigiller

On April 14, 2003, fifty years after the legendary discovery of the double helical structure of DNA by James Watson and Francis Crick, the Human Genome Project completed mapping the nucleotide sequence of human DNA. According to a Washington Post article on the subject, "the genome era of medicine offers enormous potential to improve health in the developing world by providing new insights into genetic factors that influence susceptibility to infectious diseases such as malaria, tuberculosis and AIDS" (1). As excerpted from a similar CNN.com piece, the Human Genome project has during its development "aided scientists in discovering a mutation that causes a deadly type of skin cancer and accelerated the search for genes involved in diabetes, leukemia and childhood eczema" (2). Clearly, the benefits of the mapping of the human genome are manifold. The upcoming century, which promises to be filled with all the advantages of biotechnological research and development, will undoubtedly be one of increased life expectancy and lower mortality worldwide, principally because of the conquering of the genetic frontier.

Despite the fact that the nucleotide sequencing of human DNA is nearly identical in all members of the human species, each individual has its own unique DNA fingerprint. The differences between an individual's DNA fingerprint and the general coding sequence for the species lie in "single nucleotide polymorphisms—variations in the three billion letters of the human genetic code" (2). These variations, "single changes in the arrangement of those letters that make people different…hold the key to susceptibility to illnesses such as cancer, diabetes and heart disease and individual responses to medication" (2). And in each man, woman, and children's unique DNA nucleotide sequence lays the intrinsic problem associated with the mapping of the human genome and the ease with which scientists are able to decipher individuals' DNA fingerprints. A person's genetic profile is contained in one's hair, in one's blood, in one's tissue; all of these samples are astoundingly simple to obtain. And thus, with the era of improved health and medicine as a result of the Human Genome Project, comes a certain responsibility to protect individuals' DNA sequence—an attribute so inherently personal that it must be protected at all costs.

A 2000 article by Senators James Jeffords and Tom Daschle contends that "the genetic revolution could mean one step forward for science and two steps backward for civil rights, [for the] misuse of genetic information could create a new underclass: the genetically less fortunate" (3). The American public agrees wholeheartedly that their genetic privacy should be protected. According to a Gallup poll conducted in September, 2000, 86% of adults in the United States agree that doctors should be required to obtain permission in order to handle the genetic code of an individual, while 93% surveyed affirm that their genetic information should not under any circumstances be released to research firms without express permission (3).

One of the most disquieting dangers associated with the unadulterated spread of private genetic information is that health insurance or job offerings will be denied on the basis of certain genetic predispositions that otherwise would not have been an issue. Should employers and insurance companies have the right to know the results of genetic

testing? Other related questions raised by Margaret Everett, an assistant professor of anthropology at Portland State University, include:

- Who owns genetic information?
- Do members of your family have a right to know the results of your genetic test?
- Do the police, the military, employers, insurance companies, and schools have the right to know [your genetic profile]?
- Should pharmaceutical companies "own" information about your DNA without…your consent?
- Should the possibility of economic benefit…play a role in deciding whether your DNA might be used for research?
- How should your genetic privacy be protected? (4)

These queries must be addressed in legislation. As the Jeffords/Daschle article states, "Ultimately, the greatest difficulty will be for policy-makers to strike a balance between timely promotion and use of the best genetic research and careful protection of people from genetic discrimination" (3). Clearly, genetic research cannot be abandoned because of the threat it poses to privacy; the benefits are far too great to do so. Yet the civil rights of citizens cannot be sacrificed in any way.

Legislation

A report by the Department of Labor, the Department of Health and Human Services, the Equal Employment Opportunity Commission, and the Department of Justice "argued for the enactment of federal legislation, [stating] that 'genetic predisposition or conditions can lead to workplace discrimination, even in cases where workers are healthy and unlikely to develop disease or where the genetic condition has no effect on the ability to perform work" (5). It showed that "existing protections are minimal (5)."

Thus far, remarkably inadequate legislation has been introduced on the national front. Domestically, much of the legislation is either two or three years old and has invariably been stuck in committee for months and even more. The Student Advisory Board recommends that action be taken to move these bills out of committee and onto the floor.

The single passed federal law that directly deals with genetic discrimination is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). According to www.congress.gov, the bill has "been hailed as 'taking important steps toward banning genetic discrimination in health insurance' but has also been criticized for not going far enough." The bill "prohibits a group health plan…from using genetic information to establish rules for eligibility;…it also prohibits a group health plan…from using genetic information in setting a premium contribution" (www.congress.gov). However, the Act does "not prohibit group health plans or issuers…from requiring or requesting genetic testing, does not require them to obtain authorization before disclosing genetic information, and does not prevent them from excluding all coverage for a particular condition" (5).

During the current Congress, some of these downfalls were addressed in a bill (which now sits in committee) that was introduced to the Senate called the Equal Rights and Equal Dignity for Americans Act of 2003, S.16. However, more substantial efforts

concerning genetic privacy were made the 107th Congress, a landmark year for genetic privacy legislation. Myriad bills were introduced in the House and Senate on that very subject. S.318, the Genetic Nondiscrimination in Health Insurance and Employment Act, S.318 was introduced to the Senate on February 13, 2001 by Senator Tom Daschle. This bill "would have prohibited genetic nondiscrimination in health insurance and employment" (5). S.1995, introduced by Senators Frist, Snowe, and Jeffords, would have covered the same territory as S.318. Similar was Protecting Civil Rights for All Americans Act, introduced as S.19 by Senator Tom Daschle. One record bill was S.382, introduced by Senator Snowe, which would have "prohibited discrimination in insurance" (5). In the House, the Genetic Nondiscrimination in Health Insurance and Employment Act, HR 602, was introduced during the 107th Congress as well. This was a companion bill to S.318 in the Senate. H.R. 602 would "cover all health insurance programs, prohibit enrollment restriction on the basis of predictive genetic information, ban health plans and insurers from requesting or requiring that an individual take a genetic test and prohibit health plans and insurers from pursuing or being provided information on predictive gene services" (6).

Certain legislation has also been amended to include the issue of genetic privacy. For example, the Equal Employment Opportunity Commission (EEOC) has "taken the position that the Americans with Disability Act (ADA) should be interpreted to already preclude discriminatory behavior based on genetic information" (7). Additionally, the Department of Health and Human Services (HHS) has issued regulations that will protect "the privacy of an individual's 'personally-identifiable health information' including genetic information" (7).

Consequences

Many organizations have formed with the hopes of providing support for those whose lives have already been impacted in "profound ways by the promise of genetics for diagnosis, treatment and improved health" (8). One such organization is the Genetic Alliance. The principles that the Genetic Alliance holds true are relevant to recognizing the issues of key importance in genetic privacy. Their mission statement includes the following: "Genetic conditions are universal. Every man, woman and child has some genetic predisposition, condition or disease resulting from inherited or acquired genetic changes" (8). Just as this is the statement made by the Genetic Alliance, it is the key issue in the debate concerning genetic privacy. Secondly, "Genetic information is inherently personal and must be treated as confidential and proprietary" (8). The fact that one cannot obtain his/her genetic information without undergoing tests makes the process very public; however, the fact remains that genetic information is private and must be treated so. The third point that the Genetic Alliance makes regarding the rights of citizens when it comes to genetic privacy is that "access to health care, education and employment is essential to all individuals, regardless of genetic inheritance" (8). This last point may perhaps be the most important. The fear among many concerning genetics is that if the information were to become public knowledge, one would be discriminated against due to flaws in his/her genome. Such discrimination could prevent one from getting a job, an education, or even insurance. The fact remains that if one were to be discriminated against due to his or her nucleotide sequence, it would be a direct infringement on that person's civil rights.

The Genetic Alliance gives full support of the Genetic Nondiscrimination Act and brings to the surface three points of importance regarding issues that may arise in the future. One such issue is the fact that if one feels he/she might be discriminated against due to his/her genetic information, this patient might be less likely to undergo testing vital to his/her health. Secondly, if patients refuse to offer themselves up for research, the "full promise of today's genetic discoveries will not be seen" (8). In other words, without people willing to undergo testing, technological advances will cease to be made in the field of genetics, thus putting an end to the tremendous success made thus far in the field. Finally, the exclusion of certain human beings from fields based on their flawed genetic information would create "an uninsurable and unemployable subclass at enormous financial, public, and moral cost" (8).

Recommendations

As with all scientific developments, the complete mapping of the human genome comes with tremendous opportunities as well as grave dangers. The Student Advisory Board strongly advises members of Congress to introduce and support legislation protecting Americans' genetic privacy. A compromise must be struck between the usefulness of the human genome to scientists and researchers and the civil rights granted to every citizen by the United States constitution.

References

1. http://www.washingtonpost.com/wp-dyn/articles/A7959-2003Apr21.html
2. http://edition.cnn.com/2003/HEALTH/04/14/genome.reut/
3. http://www.sciencemag.org/cgi/content/full/291/1249
4. http://www.geneforum.org/learnmore/gp/issues.cfm
5. http://www.congress.gov/erp/rl/html/rl30006.html
6. http://www.slaughter.house.gov/
7. http://www.americanbenefitscouncil.org//newsroom/genetic_keyissues.htm
8. http://www.geneticalliance.org/geneticissues/gainsurance.html

Biometrics

Tony Pilara

Biometrics is quite simply a way to authenticate a person through unique biological features. Some examples of this are fingerprint scans, retina scans, and voice recognition. As technology advances at a rapid rate, biometrics is becoming a more widely accepted way to authenticate a person. In addition to the insecurity of biometrics as a whole, there are ethical issues that pertain to the matter as well.

Already, biometrics is being used in many places. Companies are installing keyboards that allow an employee to authenticate him or herself with a fingerprint. Some laptops come with a built in fingerprint scanner just to the left or right of the touch pad. USB fingerprint scanners can be purchased to be used in the home. Gyms and other similar facilities are being outfitted with fingerprint scanners to authenticate a member and give him or her appropriate access. Grocery stores are allowing people to pay for their groceries with a fingerprint. The advantage, of course, is that they don't have to carry any money with them. ATM machines in Australia are allowing people to withdraw their money with an iris scan. With the coming of a new technology, businesses tend to assume the technology is secure, but rarely do they ask the questions.

As one might imagine, the issue of security comes into question. You can fool a fingerprint scanner even if it checks for a temperature and a pulse by having a thin coat on your own finger with the false print. Retina scanners, which scan the eye, can be followed with an accurate representation of the eye. Voice scanners can be followed by recording a sample of your subject. Voice stress analysis is ineffective because modern computers can edit the voiceprint they produce. Speech synthesizers can also use a voice pattern to produce any speech the operator wishes, fooling systems that dictate what the subject must say in order to pass as whomever he or she is. It is apparent that these new tools are not without fault.

An ethical question that is also raised is how long biometric information would be stored or what the information would be cross-referenced with. Also, what would happen if the database were to be compromised and how can users be aware of what kind of information is kept in such databases? Questions also come up about what would happen if someone fooled the system into a false "yes."

Biometrics is not a secure means for identification in its current state. Over the past few years, biometrics equipment has come down in price and the software that administers the equipment has only gotten better. Together, it is still not secure enough to authenticate a person when dealing with sensitive (financial, etc.) information. Although there is some biometrics equipment that is not easily fooled, the possibility that it can be fooled must not be ruled out. As biometrics equipment is increasing in popularity, people often fail to ask whether it is secure enough for the implementations, potentially putting the consumer data unnecessarily at risk, in many cases. Grocery stores are thinking about introducing biometric equipment to authenticate a person allowing him or her to pay for groceries without the need for money or credit cards. Banks are also allowing people to withdraw their money from an account. Until it can be proven beyond reasonable doubt that biometrics equipment is safe and secure, the author urges that no high security items (grocery stores, banks, etc.) authenticate users with biometrics

Medical and Public Records

Meredith LaSala, Priya Nand, Alexandra Frischer

Civil and Criminal Records: Information Access and Privacy

Much personal information is available through civil and criminal records. Such records are accessible at both the state and the federal level; as a result, it is necessary to examine the relevant privacy issues from both perspectives.

State Issues

States offer very easy access to a wide variety of records containing civil and criminal information. The civil records divisions contain a wealth of information about divorce proceedings, child support, real property files, financial transactions, and wills and estates. The criminal records contain detailed histories of criminal allegations, police reports, probation reports and the histories of criminal proceedings and incarcerations. These databases contain information about both individuals and corporations. With very few exceptions there are no legal barriers to accessing court files or the dissemination of the personal information with the files.

In each and every category, vast amounts of personal information can be found. When this information is assembled it can provide an extensive information profile about an individual. Personal data, driver records, addresses, employment information, and financial information can be retrieved from public databases. A vivid picture of an individual's financial history and status, personal relationships (past and present), and personal behavior can be constructed from public documents. Many times this information is not flattering or favorable. Information about other family members and friends can be obtained as well. This is easily the case when researching divorce, child support, and estate records. Children, spouses, relatives and next of kin are often easily identified.

Arrest and criminal records contain very specific information about an individual's behavior. While criminal histories are not freely given to the public, detention, probation, and arrest records are easily obtained.

Public records information is used by commercial profilers for marketing and targeted advertising. Sometimes predatory businesses utilize negative credit or bankruptcy information to unfairly target individuals who are vulnerable to pressure.

Commercial profilers will even gather data from public records and sell it back to law enforcement agencies as detailed reports. These files have been known to be inaccurate and cause severe damage to reputations and employment. In some cases these profiles can contain enough information necessary to commit identity fraud.

Federal Issues

The situation at the federal level is quite similar to the state level. Two major records access statutes govern access and release of data: the Freedom of Information Act and the Privacy Act. While access to personal information has been the focus of federal legislation in the last fifty years, the federal government has been quite explicit in attempting to protect personal information. Efforts at doing so have been prompted by the increased access of information through electronic means.

The Freedom of Information Act was initially enacted in 1966 and then later amended. It establishes the presumption that any person may access existing federal agency records on any topic. It specifies nine categories of information that may be exempted from disclosure. Disputes over access can be settled in Federal court.

The Privacy Act, adopted in 1974, establishes the right of citizens or permanent resident aliens to access personally identifiable files on themselves kept by most federal agencies. Where the individual challenges that information is incorrect, the law provides for corrections to be made.

An interesting example which highlights the privacy debate over record accessibility is the federal requirement for sex offenders to register and provide notification of their location to local and federal law enforcement agencies. Individual states are granted wide latitude to set standards and desired levels of required information. These policies set up debates around privacy and the communities' right to know when a convicted sex offender or child molester lives in their community. Debate sometimes centers on the potential threat these individuals pose to the community. At the same time, some argue that the rights and freedoms of those who have paid their debt to society and deemed fit to live in it are unfairly constrained from regaining privacy and rebuilding a normal life. The federal government through the judicial and the legislative branches has clarified the limits on registration and community notification.

With easy access to state and federal records through the Internet, it has become very easy to find information on almost anyone. Even court and arrest records can be easily accessed if one knows where and how to find them. While the two principles of privacy and freedom of information often collide today, it is important that our legislators and our judiciary constantly seek to maintain a delicate balance between them.

Since technology has made information access so easy, the Student Advisory Board proposes that personal identification information be protected in ways that will help to prevent identity fraud and abuse. Personal identification information such as a social security number should be documented on separate files that are not accessible to the general public.

As another safeguard, we recommend that those who access public records (whether for commercial, governmental, or individual use) be required to state the intended use of the information at the time of access. This is particularly significant in the access of court records, arrest records, and personal information. By requiring such a statement, violations can be better controlled. If information is misused or used in ways not stated, penalties should be imposed against the offending party.

Social Security

Background

The availability of Social Security numbers is another very important factor in the privacy debate. Social Security numbers were first created by the Social Security Act of 1935. This Act intended for Social Security numbers to be used only by the social security program. However, in 1943, President Roosevelt issued Executive Order 9393 which allowed the Social Security number to be used as a federal government identifier.

By 1961, the Internal Revenue Service used the SSN as a taxpayer ID and in 1964, the Tax Reform Act which was enacted allowed state or local tax, welfare, driver license, or motor vehicle registration authorities to use the SSN as identification. Some states use SSNs as driver license numbers and some states record this information onto databases. According to the Privacy Act of 1974, there should be a section on application forms of a disclosure notice. Many of these applications that ask for SSNs don't have this disclosure notice

To place some limit on the availability of SSNs, the federal government enacted the Privacy Act of 1974 which "limits compulsory divulgence of the social security number by government entities." However, these limits are not effectively enforced and SSNs are easily available. For example, according to the Privacy Act, there should be a section in application forms of a disclosure notice. Many of these applications that ask for SSNs do not have the disclosure notice.

As people can see, there are many problems with the Social Security Law. This personal information (SSN) that is used for plenty of things isn't safe. This personal information can lead to people stealing credit cards which result in ruining the owners credit or even death. An example is the case of actress Rebecca Schafer who was tracked down through the DMV, stalked, and killed by a fan of hers.

Recommendations

Another law should be enacted and the Privacy Act of 1974 should be stricken. The disclosure notice should be shown on every application that asks for social security numbers. SSNs should not be used as identification. There should be another number created to be used as identification which means only the Social Security Administration and federal agencies are allowed to use SSNs. It should be enacted that there will be two different numbers used for an individual.

Medical Records

The availability of medical records is of tremendous importance. Much current legislation has been introduce don this issue. The *Health Privacy Rule* took effect on April 14, 2001 under the Clinton Administration. This allows patients to inspect their own medical records while their information that is individually identifiable is protected. Any health care provider must get the patient's signature or consent to disclose their information for things such as payments, treatments and other health care options. If the patient's information is to be used for purposes that are not routine, the health care providers must receive specific authorization. Health care providers must also give every patient a written notice that tells them the permissible uses of their information.

This Privacy Rule was not met with enthusiasm by health insurers, hospitals or pharmaceutical companies. The majority feel that the privacy rule puts strict restrictions on a patient's medical information and that it will be expensive to implement in their companies. As a result, Health and Human Services has since come out with documents to assist companies and hospitals in implementing the new privacy rule. The privacy rule does not cover every entity that would have medical information on a patient. A penalty is included in the privacy rule for those who violate a patient's medical information.

The Administrative Simplification provisions of the *Health Insurance Portability and Accountability Act of 1996* were made to assist the health care industry in keeping records and claims electronically. This legislation was intended to lower the costs of administration, make information safer and decrease paperwork. This act does not apply to life insurers, researchers, employers and many public health officials. Information can be freely given to coroners, workers' compensation programs, authorized government authorities, judicial and administrative proceedings, government agencies (national security and intelligence activities). It is estimated that implementing the privacy regulation will cost $17.5 billion over the next ten years. Since then there have been slight modifications to the legislation, such as the elimination of the prior consent requirement. A draft to the privacy rule is in the making and a deadline for the rule was placed for April 2003.

As of today there is a *HIPAA Privacy Rule* that will be used by the government as the basis of privacy for individually identifiable information, consumer protection, uses and disclosure rules for health information, and allows civil and criminal penalties to be administered to violators of this privacy rule. The Student Advisory Board suggests that this new privacy rule be enforced by all government agencies. Whenever a new patient is met by a doctor, insurance agent or anyone who will handle their medical files, the patient should be notified of the rule and of their security rights. The Student Advisory Board recommends that any corporation or organization that could possibly come into contact with identifiable medical records be included under the HIPAA Privacy Rule.

USA Patriot Act

Peter Zaffaroni, Lakshmi Eassey, Jacob Gryn, Alia Salim

Background

The Patriot Act was passed less than two months after September 11th to broaden the government's ability to fight domestic terrorism by creating new federal crimes, modifying immigration laws, and increasing its ability to conduct surveillance, searches and seizures, investigations, and other activities. While the Act offers some useful policing tools, it has been broadly criticized by civil rights groups and others for eroding judicial oversight of law enforcement activities and impinging on Americans' civil liberties and privacy rights. It is recommended that the Act be amended to seek a better balance between individual rights, particularly privacy rights, and national security.

To understand the basis of criticism of The Patriot Act, it is necessary to examine it from a constitutional perspective. It is therefore necessary to provide some background on sections of the Constitution which are most impacted by the Act. The Constitution seeks to achieve several potentially conflicting goals. The purposes of the Constitution, as stated in the preamble are: to form a more perfect union, establish justice, insure domestic tranquility, provide for the common defense, promote the general welfare, and secure the blessings of liberty. One can readily see that The Patriot Act, in seeking to promote the Constitutional goals of insuring domestic tranquility and providing for the common defense through policing and surveillance activities such as wiretaps, Internet tracking, and physical searches, may undermine the goal of securing the blessings of liberty for our people. Also, our Constitutional government requires a division of power among several organs of government, where each branch --the Executive, Legislative, and Judicial-- serves to temper or balance the power of the other branches. A well informed free press, openness and disclosure are the guardians of this Constitutional system of government.

Most criticism of The Patriot Act has focused on the undue power it grants the executive branch and its erosion of Constitutional protections provided in the First and Fourth Amendments. The First Amendment provides: "Congress shall make no law…abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Whether a search or seizure is unreasonable generally depends on whether it impermissibly invades constitutionally protected privacy rights. Unless authorized under a valid search warrant, or in certain limited cases involving urgent circumstances, a search of private property or the seizure of private conversations are unreasonable under the Fourth Amendment. The warrant requirement prevents government intrusions into personal privacy in the absence of the judgment of a neutral and independent magistrate, based on the facts and evidence presented, that intrusion is justified because there is probable cause to believe an individual has committed, is committing, or may commit a crime. Also, the warrant assures that the intrusion will be limited in scope because it must specify the place to be searched and the things to be seized. It should be noted that

the Fourth Amendment protects against searches involving a physical trespass, as well as wire tapping and electronic surveillance.

There are a number of sections in The Patriot Act that are a threat to the Constitutional provisions discussed above and the Constitutional goal of securing for the people the "blessings of liberty." The most controversial provisions affecting privacy rights, and sections which should be considered for amendment, are discussed below.

SECTION 213: This section allows federal agents to conduct "sneak and peak" searches which are searches of home or office without advance notification to the tenant or property owner. It allows agents to secretly enter, conduct a search, take pictures, download computer files, etc., then leave. Delayed notice of a search is allowed if there is cause to believe that immediate notice to the property owner may have an "adverse result." The authorization of covert searches of a person's home or office conducted without prior notification contravenes the established "knock and announce" principle that normally applies when authorities execute a search warrant. Delayed notification regarding seizure of items is also permitted where the court finds a seizure is "reasonably necessary." Notice may be delayed for an unspecified "reasonable period" with "good cause extensions." Section 213 extends to all criminal investigations and is not scheduled to expire.

PROBLEMS AND AREAS IN NEED OF AMENDMENT: When notice of a search and/or seizure is delayed, one is foreclosed from pointing out deficiencies in the warrant to the executing officer, and from monitoring whether the search is being conducted in accord with the warrant. If unnoticed searches and seizures are to be allowed, it is important that the person who was the subject of the search is informed in a timely fashion. The term "reasonable period" needs to be clearly defined to require notice within a set time, such as seven days, unless the government can provide a strong counterbalancing reason to further delay the notice. Long intervals of time between government searches and notice would make it difficult to fairly contest the legitimacy of the search and seizure.

SECTION 215: This section extends the reach of the Foreign Intelligence Security Act (FISA) in terms of obtaining "any tangible things (including books, records, papers, documents, and other items)" that are being sought for an investigation "to protect against international terrorism or clandestine intelligence activities." Under FISA, the government need not satisfy the probable cause standard required for a normal search warrant. Persons whose records are obtainable under Section 215 are no longer limited to foreign powers and their agents as was once the case, but may include US citizens and lawful permanent residents. The original FISA provision which was amended by the Patriot Act required that the government specify in its application that "there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or agent of a foreign power." Although US persons may not be investigated "solely upon the basis of activities protected by the First Amendment" they can be investigated and have their personal records searched if the records are sought for an investigation involving suspected terrorism or intelligence activities. Record keepers cannot "disclose to any other person" that they released records to the FBI. Section 215 is set to expire on 12/31/2005.

PROBLEMS AND AREAS IN NEED OF AMENDMENT: This section has generated tremendous controversy, particularly as it pertains to libraries and bookstores. The government's ability to seek records from libraries and bookstores relating to the books and magazines a suspected person has read or bought could put a chill on free speech rights. Library records subject to surveillance include records of books checked out and records of Internet use. [Almanac 3/26/03] Booksellers and library personnel also feel a chill on their free speech rights because they are prevented from informing anyone, including an attorney, that they have been ordered to produce such documents. The language in Section 215 is very broad and reaches medical records, educational records and financial records. Also, although the government is required to secure a court order, the standard for issuing the order is far lower than the Fourth Amendment's probable cause standard. Section 215 states that a judge must give permission for an order if a special agent certifies that the items sought are "for an investigation to protect against international terrorism or clandestine intelligence activities." To protect privacy and First Amendment rights, a judge should determine that the person who is the target of the search is involved in some form of criminal activity, or at least make an independent assessment of evidence of wrongdoing (that may not rise to the criminal level) prior to approving an application under Section 215. If U.S. citizens and permanent residents can be the target of such investigations, there should be a requirement that the agent certifies that such persons are connected to a foreign power or terrorist organization.

SECTION 216: This section requires courts in any U.S. jurisdiction to order the installation of a pen register (outgoing calls) and trap and trace device (incoming calls) and similar techniques to track both telephone and internet "dialing, routing, addressing and signaling information" when it is certified that the information to be obtained is "relevant to an ongoing criminal investigation." Prior law required the government to obtain an order in the jurisdiction where the telephone or its equivalent was located. Now courts can issue a single order which can then be executed anywhere in the U.S. Also, this section updates the language to allow tracking of all modern communication technologies, including a cellular telephone number; a specific cellular telephone identified by its electronic serial number (ESN); an Internet user account or e-mail address; or an Internet Protocol (IP) address, port number, or similar computer network address or range of addresses. As under current law, orders cannot permit the capturing or recording of the contents of any communication. However, in the case of E-mail and Internet use, it is unclear where the line is to be drawn between content and "dialing, routing" etc. E-mail messages move together in packets that include both address and content information. Also, it is unclear whether a record of websites and web pages visited is "content". The analysis indicates that "e-mails' subject lines" and "Web search terms or the name of a requested file or article" are protected content areas. This section is not set to expire.

PROBLEMS AND AREAS IN NEED OF AMENDMENT: This section is one of the most controversial ones in the Act, particularly because there is no expiration provision. It could lead to abusive big brother government eavesdropping and snooping, and have a chilling effect on citizens' First Amendment rights to read, communicate, and disseminate information. To avoid abuse, the questions related to what constitutes "content" must be clearly defined. Also, the risk that the government may illegally or

even unavoidably eavesdrop on protected "content" in light of modern modes of communications must be addressed. Amendments must be carefully crafted in light of the state of current tracking techniques and communication technology. Modern communication technology is evolving rapidly and it would be difficult to continually assess the likelihood of government intrusion in protected "content" areas with each new technology or innovation. For this reason, it would be advisable to incorporate a sunset provision into this section of the Act.

SECTION 218: This section amends FISA's wiretap and physical search provisions. There was a distinction under the prior FISA section which required probable cause for wiretaps and searches in criminal investigations, but did not require a showing of probable cause for surreptitious foreign intelligence wiretaps and searches. The lesser standard only applied where the gathering of foreign intelligence was "the purpose of" the surveillance. Under Section 218, the lesser standard now applies even when the primary purpose of the surveillance is a normal criminal investigation, provided the gathering of foreign intelligence constitutes "a significant purpose" of the surveillance. The section will expire 12/31/2005.
PROBLEMS AND AREAS IN NEED OF AMENDMENT: Although there are legitimate grounds for lowering the probable cause standard when dealing with foreign intelligence investigations, exemptions from the Fourth Amendment warrant requirement should be narrowly defined. Allowing a lesser standard in criminal investigations that are not primarily related to foreign intelligence could lead to an erosion of constitutional protections and could give law enforcement agencies a method to circumvent the Fourth Amendment. The government should not be able to avoid demonstrating probable cause by simply alleging that the gathering of foreign intelligence constitutes "a significant purpose" of the investigation. The standard that allows warrantless searches in cases where the gathering of foreign intelligence constitutes a "significant purpose" should be made more restrictive to prevent abuse. Investigations that are primarily criminal in nature should be handled according to normal, constitutional procedures. Variance from these procedures could be allowed, but the threshold for deviation needs to be higher than Section 218 indicates. For instance, the language could be amended to require that foreign intelligence gathering be "one of the primary purposes" rather than merely a "significant purpose" of the investigation.

SECTION 203: This section authorizes the disclosure of information gathered in criminal and foreign intelligence investigations to law enforcement, intelligence, immigration, or national security personnel where such information will assist the officials in the performance of their duties. No court order is required although federal prosecutors must notify the court of the disclosure within a "reasonable time." Subsection 203 (a) permits disclosure of matters that were obtained in grand jury proceedings. Subsection 203 (b) permits disclosure of recordings of intercepted telephone and Internet conversations. Subsection 203 (d) permits disclosure of foreign intelligence obtained as part of a criminal investigation. Subsection 203 (a) is not set to expire. Subsections (b) and (d) will expire.
PROBLEMS AND AREAS IN NEED OF AMENDMENT: Some additional sharing of information between agencies is warranted and will allow legitimate investigations to

proceed more efficiently. However, because foreign intelligence surveillance does not require probable cause, sharing of information between normal law enforcement agencies and foreign intelligence authorities could be problematic. Intercepted telephone or Internet conversations containing personal information, and the broad range of material that is analyzed and reviewed by grand juries, should not be widely disseminated without a court order authorizing the disclosure. Although involving a judge in determining the appropriateness of the disclosure may cause delay in the proceedings, such delay is a small price to pay for protecting individual privacy rights. Perhaps the provisions could be amended to provide judicial oversight of the release of information unless the government has reasonable grounds to believe the sharing of information is both vital and urgent to an ongoing investigation.
Other troubling sections of the Act pertain primarily to the exercise of First Amendment rights of freedom of speech and political assembly, and the rights of non-citizens to due process, detention and removal. Privacy considerations are also involved in these provisions because the class of people subject to government surveillance and investigation will be greatly expanded.

SECTION 411: This section expands the class of immigrants subject to removal or denial of admission into the U.S. based on terrorism-related factors. Terrorism-related categories include "engaging in terrorist activity," "representing a terrorist organization," and "associating with a terrorist organization."
PROBLEMS AND AREAS IN NEED OF AMENDMENT: Although the provision seems reasonable on its face, the difficulty is the vague and poorly defined terminology. The term "engage in a terrorist activity" includes soliciting funds, membership, support and "other things of value" for a "terrorist organization", even if the organization also has legitimate humanitarian and political goals. Thus, guilt can be imposed on the basis of association with a particular organization which may openly solicit public support and have legal and worthy objectives, in addition to covert illegal objectives. The term "terrorist organization" is poorly defined. An individual accused of supporting a "terrorist organization" is free of guilt only if he or she can demonstrate "that he did not know or should not reasonably have known that the solicitation would further the organization's terrorist activity." It is not clear how one can prove they did not or should not have known that some branch or offshoot of the organization was involved in illegal activity. The terms "engage in terrorist activity" and "terrorist organization" need to be more clearly and narrowly defined to allow innocent and well meaning people to steer clear of violating this law.

SECTION 802: This section creates a new federal crime of "domestic terrorism." The crime extends to "acts dangerous to human life that are a violation of the criminal laws of the US or any state" and that "appear to be intended to influence the policy of a government by intimidation or coercion."
PROBLEMS AND AREAS IN NEED OF AMENDMENT: This new crime is too vague in its definition, and may allow government surveillance of individuals and political organizations that legitimately oppose government policies. For instance, civil disobedience and political dissent which is intended to disrupt business as usual may at times be in violation of the law, dangerous to human life (usually the life of the

protester), and "appear to be intended… to influence a policy of the government" through a form of intimidation. However, a reasonable person would not consider antiwar protesters or Greenpeace or Earth First activists engaged in civil disobedience such as blocking the entrance to buildings or camping out in old growth trees to be "terrorists." This is not to say that individuals involved in extreme forms of protest should not be subject to arrest under existing criminal laws. Indeed, arrest and subsequent publicity are often the goals of extreme protest. But, it is dangerous for the government to have license to characterize zealous protesters as terrorists. Although we would all like to see real terrorists removed as a threat to our society, we do not want to see unrestrained government action which can also threaten and undermine our free society. The crime of "domestic terrorism" should be more clearly defined so as to exclude political/environmental activists and political/environmental organizations which should not be the proper target of government surveillance and privacy violating operations. The Patriot Act's passage in September 2001 was strongly supported in both houses of Congress. More recently, however, some lawmakers have expressed concern over certain provisions of the act and have initiated new legislation intended to curb or modify the powers they grant.

Subsequent Legislation

Representative Bernie Sanders (I-VT) intriduced the Freedom to Read Protection Act (HR 1157) which seeks to exempt libraries and bookstores from Section 215 of the Patriot Act and amends the Foreign Surveillance Intelligence Act of 1978 to read, in part:

> "The Director of the Federal Bureau of Investigation or a designee of the Director…may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

With respect to libraries and bookstores, this provision allows for officials to demand the purchase or borrowing records of any individual for reasons of national security. Investigators need make no formal criminal charge against the individual, nor need they obtain a traditional warrant (rather, warrants are obtained from judges on the secret Foreign Intelligence Surveillance Court). Additionally, the librarians and bookstore employees compelled to produce the records are bound by a gag order and thus cannot inform the patron involved that s/he is under federal investigation.

Proponents of this extension of investigative power maintain that it is a valuable and worthwhile tool in identifying potential terrorists. They additionally point to the fact that the act does not allow the new powers to be used in investigations "conducted solely upon the basis of activities protected by the first amendment," meaning that any search must be driven by concern for national security. For example, Department of Justice spokesperson Mark Corallo, for example, sees little threat to the average citizen. "We don't have any interest in looking at the book preferences of Americans," he said. "We don't care, and it would be an incredible waste of our time" (Chicago Tribune).

Library and book industry spokespersons, on the other hand, object strongly to being required to give up their records on demand and fear that even the possibility of investigation may discourage some people from reading freely about topics that might cause government suspicion. In a formal resolution, the American Library Association stated that it "considers that sections of the USA PATRIOT ACT are a present danger to the constitutional rights and privacy rights of library users" (ALA). Chris Finan, President of the American Booksellers Foundation for Free Expression, similarly stated that "The Patriot Act gives federal authorities virtually unchecked authority to search our customers' records and raises concern that government is monitoring what people are reading" (ABFFE).

It is this concern over "unchecked authority" and a belief in the necessity of more clearly demonstrating probable cause that prompted Rep. Sanders to introduce HR 1157. "The person whose records are being searched by the FBI can be anyone," he said in a March press conference. "The FBI doesn't even have to say that it believes the person is involved in criminal activity or that the person is connected to a foreign power. This is not acceptable. The legislation we are introducing today will go a long away in protecting the basic freedoms of every American."

The fact that the DOJ will not release the number of people whose library or bookstore records have been seized under the provisions has further increased criticism of the Patriot Act. Despite the DOJ's claim that releasing specifics about the implementation of certain powers granted by the act would constitute a threat to national security, several organizations, including the American Civil Liberties Union and the Electronic Privacy Information Center, have filed lawsuit in order to obtain more information. While not directly tied to HR 1157, the lawsuit demonstrates the common concern over the reach of Patriot Act powers and the relative lack of details available on how they are being used.

Recommendation

The Patriot Act is a large and complex law that was passed by Congress with little debate during a stressful period of our country's history. Although many sections are useful and appropriate, others are a threat to some of the fundamental constitutional values that define our nation. Congress must begin the hard work of formulating appropriate amendments to bring the Act into better balance with our three branch system of government and with the "blessings of liberty" guaranteed by our Constitution.

Surveillance

Jessica Hartzell, James O'Connell, Hale Reynolds, Roger Kopfman

Ever since September 11, 2001 the United States has been in a state of heightened security. Some of it, such as the increased security in public transit and airports, and increased coast guard patrols of the nation's ports and waterways is very apparent to everyone. Many of the most widespread security measures, however, are not. With these visible forms of security surveillance programs have been implemented to monitor internet and telephone traffic, in order to catch potential terrorists before they act. The question now is, are they worth it?

Carnivore

Carnivore is a surveillance tool used by the FBI. It breaks into the network or individual computer that it is directed to and gives the FBI access to everything on that machine or network. While this seems like a tool that could easily be abused, the Senate has set strict regulations on when it can be used and it has a committee that makes sure the regulations are obeyed. To use Carnivore, the FBI must get a court order, much like a search warrant. They must have probable cause and it can only go into specified machines, nothing more.

Echelon

Like Carnivore, Echelon is a surveillance tool. It is a system of computers all around the world working together that tries to intercept every e-mail, phone calls, fax, and telex. Each set of computers has a fixed key-word list to look for from the top intelligence agencies of words, and some specific to the region word lists. If it finds one or more of the key-words, the intercepted message is sent to a human analyst to check out. It is mainly done through the US, Canada, Germany, Great Britain and Australia even through others are involved

Pro

- Efficiency in monitoring internet traffic.
- Monitoring may result in greater homeland security.

Con

- Possible for the FBI to monitor those who have not been served a court order (violation of Fourth Amendment)
- The ACLU believes Carnivore is Unnecessary, violates the fourth amendment and comes at a time of record wire tapping
- The question we are left with is this; Is the united states at a great enough risk to allow this kind of blatant infringement on privacy to occur?

Analysis

Carnivore can be used effectively to monitor traffic and ignore irrelevant pieces of information. It is strictly regulated by the Senate, and information about the program is available to all citizens. There is a possibility that, had there been an alert and surveillance of international communication, perhaps thousands of lives would be saved. Therefore we believe that Carnivore is a necessary tool for the safety of the United States.

Echelon, from the limited information we can gather, is also an effective tool in monitoring communication and (hopefully) preventing terrorist attacks. The lack of regulation and available facts about the program however make the Echelon program a very dangerous infringement on the fourth Amendment. By allowing this program to be used in our country we are losing, possibly permanently, our privacy in order to protect it.

Registration of Muslim Immigrants

Chris Curd and Derek Lipkin

Background Information

"Special Registration" is a system that will let the government keep track of non-immigrants that come to the U.S. every year. Some of the approximately 35 million non-immigrants who enter the U.S. -- and some non-immigrants already in the U.S. -- will be required to register with immigration authorities either at a port of entry or a designated immigration office in accordance with the special registration procedures.

These special procedures also require additional in-person interviews at an immigration office and notifications to immigration authorities of changes of address, employment, or school. Non-immigrants who must follow these special procedures will also have to use specially designated ports when they leave the country and report in person to an immigration officer at the port on their departure date. Under this program enacted by the INS (currently the Bureau of Citizenship and Immigration Services, or BCIS), all male immigrants from the following twenty countries are forced to register with the BCIS or face deportation:

-Afghanistan
-Algeria
-Bahrain
-Bangladesh
-Egypt
-Eritrea
-Indonesia
-Jordan
-Kuwait
-Lebanon
- Morocco
-North Korea
-Oman
-Pakistan
-Qatar
-Saudi Arabia
-Somalia
-Tunisia
-United Arab Emirates
-Yemen

To comply with this program, a foreign-born man from one of the selected countries must appear before a BCIS clerk and is asked for his parents' names and addresses, the names and addresses of American contacts, his e-mail address and a form of identification other than his passport and immigration document. He is also digitally photographed and fingerprinted, with both the picture and the prints run immediately against various criminal and immigration service databases. He is also asked how he arrived in the United States and when, as well as whether he has any connection to terrorist organizations.

Obviously, this is a violation of a person's rights and assumes that they are guilty until proven innocent. It also contributes to provoking violence against immigrants from these countries, as they will largely be stereotyped as "terrorists." Despite the fact that it is an infringement of people's rights, the BCIS believes this program is necessary for the defense of our country and preserving national security.

\

Legislation

During the 108th Congress, various acts have been introduced on the subject of registration and immigration. Over the years, these two areas have been discussed and debated by many, especially after the events of September 11 and the subsequent War on Terrorism.

The Student Advisory Board, in its research, came across several acts that pertain to civil liberties, as they pertain to the issue of privacy in the United States. The most inexcusable proposals came within the "Immigration Security and Efficiency Enhancement Act of 2003," introduced to the House of Representatives by Mr. Baca, along with several other representatives.

Section Four of this document outlines the "Establishment of Electronic File Management System." This proposed system is a "computer network composed of state-of-the-art electronic file management system and computer information system to efficiently receive and process files submitted electronically, detect incorrectly filled applications and forms, and securely share inflation within the network."

This is a blatant invasion of privacy, as it is essentially a government funded system in order to categorize and file the information of every single citizen in the United States. Therefore, it is not merely for immigration, but for the entire country, affecting every citizen.

Also, Section Five, named the "Establishment of Immigration, Refugee and Asylum, and Naturalization Filing System through Certified Service Providers," outlines a system which "provides for the electronic filing and submission of applications only from organizations and entities certified by the department to perform immigration and naturalization services on behalf of applicants." This has a major loophole, as government can certify any organization, allowing it to gain information on immigrants through the organization. Therefore, it is able to access unknown amounts of information, if necessary. This takes the decision to have information available out of the hands of the individual citizen, and into the hands of the United States government.

After a close evaluation of this act, the recommendation made by the Student Advisory Board is to work against this and any other bills that coincide with this proposal. Privacy should still be a decision the individual citizen is involved in, and therefore, the Federal government has no right to make the decision. The Fourteenth Amendment defends the civil rights of all citizens, and therefore, this act is plainly unconstitutional. The issue of registration and immigration needs to be present before the people of the United State before any further action is taken.

Conclusion

Christina Rosenberg, Vice-Chair

On behalf of this year's Student Advisory Board, I would like to thank you for considering our findings and recommendations. When we first started working together last October, our interests for the annual topic ran everywhere from bovine rights to abortion to environmental polices and back again; yet no one could deny the growing importance of the issue of privacy as it pertains to civil liberties. With the advent of the internet, the tragedy of September eleventh, and a number of other changes in American society today, we found that the privacy of American citizens is being jeopardized more and more. What we have shown you is only a mere sampling of the many issues and questions that currently revolve around privacy.

We hope that you have gained a better understanding of what kind of information is out there, what is being done with it, and what can be done with it. The past eight months have been an invaluable learning experience, not only teaching us to research and learn about past and present privacy legislation, but also giving us a glimpse into how an issue such as this affects everyone from high school students, to companies, to a nation. We would like to thank Congresswoman Anna Eshoo again for the opportunity and experience she offered us, and to all of you for coming to hear the knowledge we have gained from it.

2003 Student Advisory Board Members

Nik Warrior, Chair	Bellarmine College Preparatory
Christina Rosenberg, Vice-Chair	Menlo School
Christopher Curd, Secretary	Bellarmine College Preparatory
Derek Lipkin, Technology Officer	Los Altos High School
Elizabeth Ashton	Los Altos High School
Esen Boyacigiller	Castilleja School
Nicholas Deming	Bellarmine College Preparatory
Zayra Diaz	Woodside Priory School
Julia Duncan	Woodside Priory School
Lakshmi Eassey	Palo Alto Senior High School
Hilary Englert	Menlo-Atherton High School
Derek Fletcher	Los Altos High School
Alexandra Frischer	Woodside High School
Jacob Gryn	Woodside High School
Lauren Habig	Sacred Heart Preparatory
Jessica Hartzell	Half Moon Bay High School
Roger Kopfmann	Menlo-Atherton High School
Meredith LaSala	St. Francis High School
Priya Nand	Woodside High School
James O'Connell	Half Moon Bay High School
Danielle Paya	Notre Dame High School
Anthony Pilara	Sequoia High School
Preeti Piplani	Los Altos High School
Liesl Pollock	Castilleja High School
Margaret Ren	Castilleja High School
Hale Reynolds	Woodside High School
Helen Rhee	Monta Vista High School
Alia Salim	Los Altos High School
Kalpana Sundaram	The Harker School
Elizabeth Tafeen	Notre Dame High School
Grant Toeppen	Sacred Heart Preparatory
Daniel Wenger	Woodside Priory School
Michael Yost	Woodside Priory School
Peter Zaffaroni	Woodside Priory School