PRIVACY & AMERICAN BUSINESS
A Comprehensive Report and Information Service

Introducing *P&AB's* Inaugural Electronic Issue

Volume 8 • Number 3 August 2001

Slaughter Supports Genetic Privacy

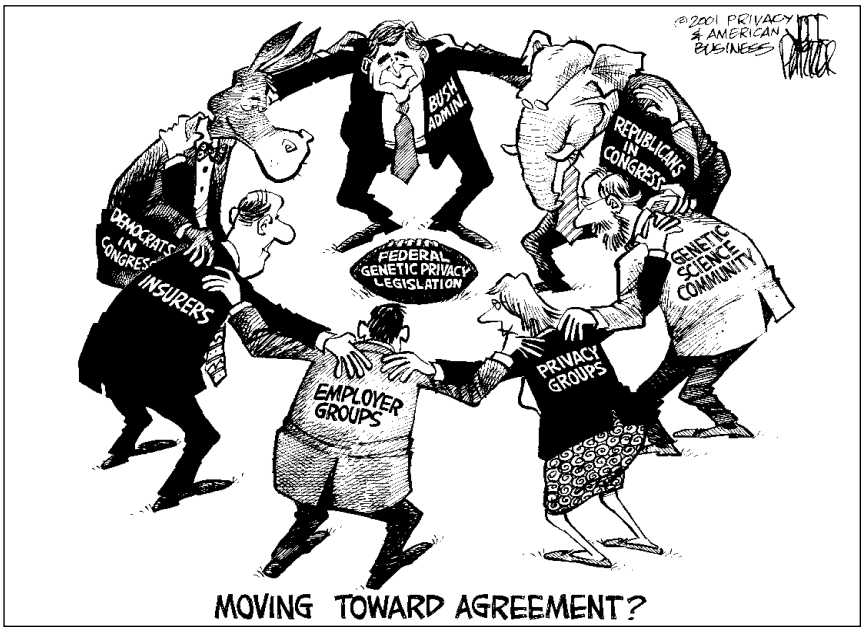
Privacy of genetic information has been in the news a great deal and gained significant momentum over the past six months. I want to outline for readers of ***P&AB*** the stakes in the genetic privacy debate, review my legislation on this issue and provide an idea of what I expect to see in the next six months.

Rep. Louise Slaughter (D-NY)

Weighing the Stakes

It is not an exaggeration to say that every American has a stake in the genetic privacy debate. Every human being carries genetic mutations that may predispose him or her to illnesses like cancer, heart disease and diabetes. Having said that, however, simply having a gene is no guarantee that one will ever get sick. Genetic mutations only increase or decrease the risk of disease. Our understanding of those risks remains poor and we have little more knowledge of how genes interact with

Continued on page 3



ISSUE AT A GLANCE

Privacy & American Business
Two University Plaza, Suite 414 Hackensack, New Jersey 07601
Tel. 201.996.1154 Fax. 201.996.1883 Email. ctrslr@aol.com

PRIVACY & AMERICAN BUSINESS
A Comprehensive Report and Information Service

Alan F. Westin
Publisher and Editor
Robert R. Belair
Editor
Lorrie Sherwood
Executive Editor

Privacy & American Business (ISSN #1070-0536), an activity of the Center for Social & Legal Research, is published bi-monthly from Two University Plaza, Suite 414, Hackensack, N.J. 07601. Phone 201-996-1154, FAX 201-996-1883, email: ctrslr@aol.com or pab@idt.net Website: www.pandab.org and www.PrivacyExchange.org. Subscriptions are $395 annually; additional subscriptions within a subscriber organization are $120. Special rates are available to cooperating organizations. Third class non-profit postage is paid at South Hackensack, N.J. and other locations, Permit #599 and 6174.

P&AB's ***New Look***

We're pleased to bring you ***P&AB's*** Inaugural Electronic Issue. We think that in a world of high-speed news cycles and expanding privacy issues, the time is right. This new format will mean a more timely monthly report for our subscriber at the desktop. And, as you would expect, it will be filled with the information you want and the analysis you need to help you better understand and operate successfully in this new privacy-hot climate. We hope you like it and will find some of our new features and departments especially useful, like the books and resources you'll find on pages 13-15. We'd like your feedback, so call me a buzz at (201) 996-1154 or shoot me an email at ctrslr@aol.com on your ideas and suggestions.

"Managing the Privacy Revolution 2001" Bigger, Better … and Different

The Eighth Annual National Conference is in the works for Washington, D.C. at the Renaissance Hotel. This year, when they say, "It's not just another privacy conference," it's more than hyperbole! Save November 27 for the CPO and Privacy Practitioners' Workshop, November 28-29 for "Managing the Privacy Revolution Conference 2001" AND the new **Privacy Expo 2001. Privacy Expo 2001** will offer attendees an exhibit hall of important new privacy software, hardware, tools and consulting solutions within the most respected annual privacy event of the year. Those interested in exhibiting should contact me at 201-996-1154. Exhibit space is limited.

The conference topics will again be cutting edge. The major players on the privacy stage from business and government, the U.S. and abroad, will be on hand as keynoters, speakers and panelists. We hope you'll be there too. Look for an exciting announcement about "Managing the Privacy Revolution 2001" in your inbox and mailbox.

P&AB ***CPO Program Plans for 2002***

P&AB's CPO Program is planning for 2002. If there's something you'd like to see on the agenda for 2002, let us know.

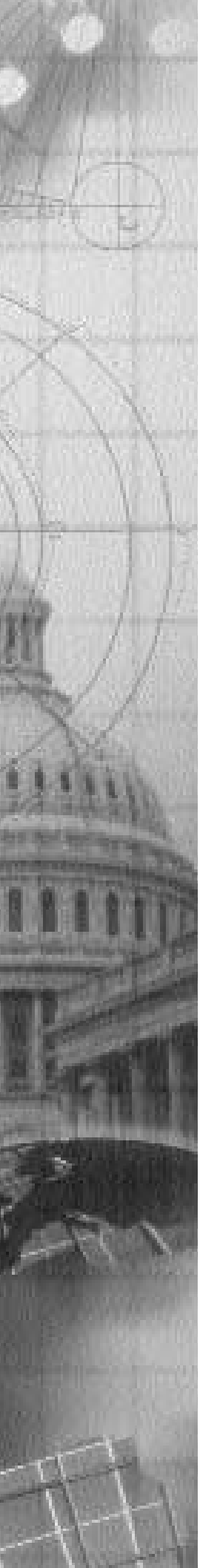
ACPO/POA Merger Approved

The merger of The Association of Corporate Privacy Officers (ACPO) and the Privacy Officers Association (POA) has been approved. This merger will create a single, strong cross-industry organization devoted to the development and interests of the privacy officers profession. More details will follow.

DMA Seminars 2002

The Direct Marketing Association, with its strong record of keeping its members ahead of the privacy curve, and ***P&AB*** joined forces to present "Balancing Privacy, Practices and Profits," July 11-12 in NYC to a full house. The two-day expert briefing and seminar focused on helping marketers learn to survive privacy storms and manage privacy issues effectively. The program scored high and plans are now afoot to take a new Seminar to marketers in Chicago and Washington, D.C. in 2002. Watch for details in my future From the Executive Editor.

Lorrie Sherwood
Executive Editor



Continued from page 1

each other or with environmental factors like diet, smoking or exposure to chemicals. While we all face this common genetic challenge, there are also very real stakes for specific groups and interests. Some of the major stakeholders who have particular concerns that we must consider in this debate include:

Employers

Regardless of whether your company has any active interest in the genetic makeup of its employees, the corporation has a major stake in the genetics debate. Many employers come into possession of employees' genetic information, whether they seek it or not. Employers must decide how to maintain, share and protect that information. In some cases, employers have expressed interest in performing genetic tests on workers. We must, as a society, determine when such genetic tests are acceptable and when they should be prohibited. If employers are not active participants in this debate, they risk ending up with an unacceptable or unworkable proposal.

Scientists

Scientists have enormous concerns about genetic privacy. Researchers tell me that it is increasingly difficult to recruit patients to participate in genetic research, largely because those individuals are desperately anxious about the privacy of their genetic information. In the absence of laws to prevent genetic discrimination, many Americans are simply deciding that the risk is too great. As a result, we are in danger of failing to realize the tremendous promise of genetic research.

Healthcare Providers

Healthcare providers need access to genetic information and patients need to be comfortable disclosing this information to them. However, I receive letters regularly from individuals saying they are afraid to discuss even a family history of disease with their doctors because they fear that this information may end up in the hands of their insurance company or employer.

Individuals

Everyone has a personal stake in this debate. We all have flawed genes and many of us can name a disorder that runs in the family. Today, however, many Americans are deciding not to take genetic tests, denying themselves valuable information about their health for fear of discrimination. We do not want to force our children and grandchildren into this same Catch-22, where taking a genetic test puts us at risk of discrimination, while not taking a test may obscure valuable opportunities for preventing disease.

> Individuals say they are afraid to discuss a family history of a disease with their doctors

Why H.R. 602?

With the advent of genetic research, I realized that we were standing on the frontier of a totally new way of practicing medicine. I recognized the potential for discrimination that would exist when we could examine an individual's DNA and identify potential future health risks.

In late 1995, I introduced the first bill to ban genetic discrimination. Today, I am proud to sponsor H.R. 602, the Genetic Nondiscrimination in Health Insurance and Employment Act, a bill that has earned the steadfast support of my original co-sponsor, Rep. Connie Morella (R-MD) and over 250 bipartisan co-sponsors, well over a majority of the House. In the Senate, identical legislation (S.318) is sponsored by Majority Leader Tom Daschle (D-SD), Sen. Edward Kennedy (D-MA) and over 20 other Senators. Our legislation has been endorsed by over 300 organizations that care about healthcare issues.

> We are standing on the frontier of a totally new way of practicing medicine

Briefly, the provisions of this legislation, with regard to health insurance, would:

- cover all types of health plans, including both state and federally-regulated
- prevent health insurers from denying, canceling, refusing to renew or changing the terms of, premiums or conditions of coverage based on genetic information
- bar insurers from requesting or requiring that a person take a genetic test, or reveal the results of genetic tests
- prohibit health plans from pursuing or purchasing predictive genetic information.

In employment, the bill would:

- apply to employers, unions, training programs and agencies
- prohibit the use of predictive genetic information to make employment-related decisions, including decisions about hiring, firing and promotions
- ban employers from requesting or requiring that an individual take a genetic test, except in limited circumstances like monitoring toxic exposures
- require that predictive genetic information be maintained in a confidential fashion and disclosed only with consent, or to researchers complying with strict privacy standards.

My fellow sponsors and I believe our bill represents a simple, common sense approach to banning unfair genetic discrimination. Over time, however, we have fielded many questions about the specific impact of the bill. I would like to address some of the most common questions and misconceptions about this legislation.

The bill would require that employers have certain privacy protections in place. The legislation states that genetic information shall be treated or maintained as part of the employee's confidential medical records. Genetic information is personal, private and permanent, and it should be treated as such. If predictive genetic information is released without authorization, the result could be devastating to the employee and to his or her family members. I firmly believe it is reasonable to require that access to genetic information be limited.

The bill would establish serious penalties for violations. It is not enough for Congress to politely encourage companies to keep genetic information private. There must be a meaningful incentive to do so, including stiff penalties for those who break the law.

This legislation would not prohibit employers from operating wellness programs. There is a specific exemption in the bill for such programs as long as they are voluntary and any genetic information is provided only to the employee.

My bill would not make employers liable for innocent acquisition of genetic information. The legislation provides a safe harbor for employers when they come into possession of genetic information they have not sought.

This initiative would not require businesses to hire new personnel to administer its requirements. This bill would not require a business to bring a new person on board just to handle genetic information, but would allow for reasonable overlap so long as privacy and nondiscrimination policies are followed.

The sponsors of this bill have worked hard to be aware of the wide variety of business environments. We have discussed this legislation with many different employers and interests. It is our conviction that we have crafted a responsible compromise that balances the rights of individuals with the needs of business.

Current Action in Congress

Over the past months, Congress has seen a surge of interest in genetic nondiscrimination. In fact, after over five years of inaction, I admit that it has been something of a shock to see three hearings on genetic discrimination held in July.

In early June, the shift of power in the Senate administered a major boost to our efforts when the sponsor of S. 318, Sen. Daschle, became Majority Leader and took control of the Senate schedule. On June 23, President Bush called for genetic nondiscrimination legislation in his weekly radio address. On July 11, the House Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection held a hearing on genetic discrimination in health insurance. On July 24, the House Education and the Workforce Subcommittee on Employer-Employee Relations held a hearing on genetic discrimination in employment. And on July 25, the Senate Health, Education, Labor and Pensions Committee wrapped up its hearing on both these issues. (See box below.)

When Congress returns from the August recess, I predict that markups of this legislation will occur fairly rapidly. I very much hope to see this bill on the House floor before Columbus Day.

In the genetics debate, we face challenges as employers, workers and patients. The passage of genetic nondiscrimination legislation will undoubtedly be just the first of Congress' forays into the ethical and policy considerations raised by new technology.

I hope the readers of ***P&AB*** will agree that H.R. 602, the Genetic Nondiscrimination in Health Insurance and Employment Act, is a balanced, workable solution to this challenge, crafted with input from all the stakeholders. I intend to continue working with all the interested parties to ensure that no one suffers discrimination simply because they have a genetic predisposition to disease.

Editor's Note: This is an excerpt of a speech that was prepared for delivery by Rep. Louise Slaughter (D-NY) at ***P&AB's*** CPO Washington Briefing and Peer Workshop. Because of her legislative schedule, the speech was delivered by an aide. ■

July 11, 2001

House Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection hearing on "The Potential for Discrimination in Health Insurance Based on Predictive Genetic Tests."

http://energycommerce.house.gov/107/hearings/07112001Hearing322/hearing.htm

July 24, 2001

House Education and the Workforce Subcommittee on Employer-Employee Relations hearing on "Genetic Non-Discrimination: Implications for Employers and Employees"

http://edworkforce.house.gov/hearings/107th/eer/genetic72401/wl72401.htm

July 25, 2001

Senate Health, Education, Labor and Pensions Committee hearing on "Fulfilling the Promise of Genetics Research: Ensuring Nondiscrimination in Health Insurance and Employment"

http://www.senate.gov/~labor/107hearings/july2001/072501wt/072501wt.htm

Consumer Privacy in the States

With the exception of ten major legislatures still at work, the states have either completed their legislative sessions (as of August) or have adjourned until 2002.

Consumer privacy issues continue to be an item of major interest and activity on the part of state legislators. More than 7,000 privacy bills were introduced in 2001; 800 relate to medical privacy alone. Republicans and Democrats in the legislatures, as well as state attorneys general and governors, are also looking closely at financial privacy, insurance, marketing, credit and identity theft.

More than 7,000 privacy bills were introduced - 800 relate to medical privacy alone

SO FAR IN 2001

GLB

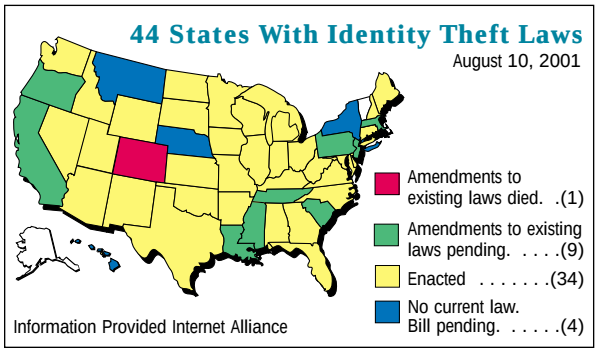
Before Gramm-Leach-Bliley (GLB) was enacted in 1999, states had the exclusive right to regulate the insurance industry, or any other industry in their jurisdiction (not pre-empted by federal legislation). With GLB, states are required to enact insurance privacy laws or regulations by July 1, 2001. Most states, but not all, as of mid-2001 have put laws in place that will allow for permanent regulations.

In doing this, some states have followed GLB, while others have gone beyond, requiring consumers to "opt-in" before health information is shared, as the NAIC model provides. Arizona, Florida, Louisiana, Montana, Washington, Wisconsin and Wyoming all have enacted an "opt-in" requirement for health or medical information. States leaning toward "opt-in" for health are Kansas, Mississippi, New Hampshire and Rhode Island. Vermont came close to repealing its financial "opt-in" law, while North Dakota has moved to "opt-out."

Financial institutions in North Dakota are exempt from the state's "opt-in" law if they comply with GLB. In June, the FTC found that North Dakota's law is not inconsistent with GLB, therefore the state law was not preempted under Section 507 of GLB. This decision confirms that, for the states, GLB provides "a floor" or minimum protection for consumer privacy, and this can be exceeded by the states.

Health

In June, Texas enacted the "Texas Medical Privacy Act." It gives consumers the right to inspect their health records and prohibits employers from seeing employee health records, except when it is essential to employee job performance. This law also forbids health organizations from sharing patient information, including prescription drug information, with marketers and advertisers. Patients may sue, but not for punitive damages, while the AG may impose penalties of $250,000 per violation. (An employer who violates the Texas medical privacy rights of employees could obviously face very high recoveries if multiple violations are found.)



Zoom-in on map for viewing.

Presented at ***P&AB's*** CPO Washington Briefing and Peer Workshop on July 25-26 by Emily Hackett, Internet Alliance

In a controversial move, Hawaii repealed its medical privacy law, the "Privacy of Healthcare Information Act," due to go into effect this year after being suspended in August 2000. The law, which included criminal sanctions, was heavily criticized as too stringent, confusing and costly. Supporters of the repeal this year said that the law was unnecessary in light of the HIPAA Regs, even though those will not take effect until 2003.

During June and July, the Governor of Rhode Island signed two bills, S.B. 803 and H.B. 5347, prohibiting health plans, health providers and insurance administrators from releasing genetic information without prior written authorization. Earlier this year, South Dakota enacted laws restricting the use of genetic tests by insurers and employers: H.B. 1003, H.B. 1050, S.B. 1 and S.B. 2.

Oregon repealed its unique law on uses of DNA information, which granted all people property rights to their DNA data. Because the law would give individuals the right to control how their DNA might be studied, even after many years, it was felt that this would hinder scientific research. The new law, S.B. 114, requires informed consent before the use of DNA is permitted and provides privacy and discrimination protection for both individuals and their relatives. South Dakota, Arkansas, Louisiana, Maryland and Nebraska also enacted genetic privacy laws this year.

Marketing

Twelve states passed laws regulating telemarketing in 2001 with more pending. Virginia enacted the "Virginia Telephone Privacy Act" which, apart from creating a "Do-Not-Call" list, bans all calls before 8:00 a.m. or after 9:00 p.m. The law also prohibits telemarketers

from using devices which block caller ID, and requires that all callers give their own name and their business. The law allows the AG, any Commonwealth Attorney and any attorney for a county, city or town, as well as individuals to sue for damages and legal fees. Other states which enacted similar "Do-Not-Call" laws in 2001 include: Arizona, Colorado, Indiana, Louisiana, Maryland, Montana, Nebraska, Nevada, Oregon, Texas and Wyoming.

In April, Virginia also enacted H.B. 1141, which requires paid telemarketers making calls on behalf of a candidate running for office to identify the candidate, campaign committee or any other organization making the call.

In June, Illinois enacted S.B. 333, providing that personal information in an insurance policy is owned mutually and exclusively by the insured and the company. This includes name, address, the value of the policy, inception, renewal and expiration dates, as well as other personal information. No other entities may use the information for marketing purposes without the insurance company's written consent.

In July, Louisiana's Governor signed S.B. 703 which prohibits supermarkets from selling or sharing any information they receive from the use of discount or membership cards.

Workplace Monitoring

In July, Delaware enacted H.B. 75, an employee privacy law which requires employers who monitor their employees' telephone calls, e-mail or Internet usage to notify employees before doing so or at the time of hiring.

Commerce

Louisiana enacted H.B. 626, a consumer privacy law that will affect all credit card transactions in the state. Merchants cannot print out any part of the credit card number, or the expiration date, except on the receipt given to the customer. Then, only the date and last 5 digits may appear. Merchants may be liable to customers and credit card issuers for damages, expenses and attorney's fees if consumer credit card information is used improperly. The law takes effect Jan. 1, 2002 for new machines and Jan. 1, 2004 for old ones. It does not apply to copies made where the only means of recording the number is by hand or imprinting the card.

DMV Records

In June, New Hampshire's Governor signed H.B. 590, a bill preventing life insurers from accessing an individual's motor vehicle records without written consent and assurance that the record would be used only for insurance purposes. Insurers cannot require consent for the release of personal information as a condition of doing business. The law takes effect August 28, 2001.

South Dakota and West Virginia have both acted to limit the use of driver's records. The South Dakota law, "An Act to Prohibit the Disclosure and Use of Personal Information Contained in Certain Motor Vehicle Records," H.B. 1045, is an "opt-in" law. Social Security Number, name, address, telephone number and medical or disability information cannot be disclosed without prior consent. This does not include information relating to previous car accidents, driving violations or registration status. There are limited exceptions, including one allowing insurers to inspect records in connection with claims investigating anti-fraud activities, rating and underwriting. West Virginia also enacted H.B. 2256 this year, a similar "opt-in" law for DMV records.

Identity Theft

In June, Florida made identity theft a felony. Specifically, H.B. 1845 provides that the willful and fraudulent use of another's personal identification information is a 2nd degree felony. Many other states have ID theft bills pending (see below).

BILLS TO WATCH

Financial Privacy

The California legislature is still considering a very important financial privacy bill, the "Financial Privacy Act of 2002," S.B. 773. If passed, the law would require that financial institutions provide notice and get prior consent before disclosing or sharing any confidential consumer information with a third party. This law would also require that consumers be given the opportunity to "opt-out" of having their information shared with affiliates. Information that could not be shared unless the consumer "opts-in" include customer status, account information, payment history, purchases, consumer report information and information obtained through an Internet "cookie" or web server. This bill passed the Senate in June, was approved by the Assembly Committee on Banking and Finance, and is currently in the Judiciary Committee.

Identity Theft

California State Sen. Debra Bowen (D) has proposed an identity theft bill, S.B. 168, to allow consumers to place a "security alert" or a "security freeze" on their credit reports. A security alert would notify all credit report users that the consumer has been the victim of identity theft. It would have to be placed on the report by the credit reporting agency within five business days and would remain in place for at least 90 days, pending renewal by the consumer.

The "security freeze" would prohibit a credit reporting agency from releasing any information from a credit report without the consumer's permission (with some exceptions). Third parties can, however, be advised about the existence of a freeze. The credit reporting agency would also have to provide the consumer with

an ID number to "unfreeze" the report or authorize the release of information. The freeze would remain in effect until the consumer "unfroze" the report by making the request through certified mail. If passed, the law would take effect July 1, 2002. This bill has passed the Senate and is currently in the Assembly.

New York's Senate Majority Leader, Joe Bruno, is pushing an identity theft bill which would criminalize possession of another person's individually identifiable information with the intent to obtain credit, goods, money or property without permission. The bill passed the Senate and is in the Assembly Committee on Codes (S.B. 694, A.B. 3648).

Telecommunications

Minnesota is currently considering a law, S.B. 565, to prohibit telecommunications providers from disclosing customer information to third parties without express prior consent. Customer information includes individually identifiable information, such as phone calls made and received, length and date of calls, account balances, payment history and other information the provider may have. The individual's phone number and address, if published in a directory, do not apply unless the customer has requested that they be unlisted. The bill is currently in the Senate Committee on the Judiciary.

Marketing

California, Illinois and Ohio all have bills still pending, which would mandate the creation of statewide "Do-Not-Call" lists (S.B. 17, H.B. 176 and H.B. 199).

SUMMING UP

Despite passage of GLB and impending federal HIPAA regulations, which set out major federal privacy rules for the financial and health sectors, the readiness of state legislators to propose and enact broad new consumer privacy protections remains high in 2001, and beyond. Analysis of the state legislative voting patterns shows that this outlook is shared by both Republicans and Democrats, and conservatives as well as liberals. And, all types of states are taking these actions, large and small, and in all regions.

> The readiness of state legislators to propose and enact broad privacy protections remains high in 2001

In this charged climate, working to block extreme proposals, and helping to write privacy laws that make consumer notice and choices the key dynamic, represents a major priority for the American business community. ■

Consumer Privacy Litigation Rising Due to Plaintiffs' Bar, FTC and AGs

One of the hottest subjects in the consumer privacy arena is litigation. According to ***P&AB*** President & Publisher, Alan Westin, consumer privacy litigation has blossomed in the last two years for three reasons. First, private plaintiffs have increasingly brought privacy class action suits under new federal and state legislation and theories of consumer reliance on company privacy policies. Second, the Federal Trade Commission (FTC), which has begun to exert greater influence in the privacy area, has brought actions against online companies for alleged "false and deceptive" practices. Finally, the increase in consumer privacy litigation can be attributed to state attorneys general, who are bringing suits under state consumer protection laws.

Since September 2000, ***P&AB*** has monitored consumer privacy litigation to keep privacy officers and their organizations informed of emerging legal trends in the consumer privacy arena. In its *Bimonthly Report on Consumer Privacy Litigation*, ***P&AB***:

- Monitors lawsuits when they are filed
- Tracks the progress of litigation by giving updates on pending cases
- Provides analysis and commentary of the claims.

The *Report* is an exclusive benefit of membership in ***P&AB's*** CPO Program. Currently, it tracks consumer privacy litigation in eight categories: 1) obtaining personal information by misrepresentation or fraud; 2) disclosing customer/user information in violation of promises; 3) tracking or monitoring Internet users without permission or disclosure; 4) using personal information for improper purposes; 5) actions by state regulatory agencies (other than attorneys general and consumer protection agencies); 6) other consumer privacy litigation of interest, including suits between companies; 7) business lawsuits challenging consumer privacy laws and regulations; 8) actions for sending unsolicited fax advertising.

To date, ***P&AB*** has compiled information on 65 consumer privacy cases. These suits were brought against 67 corporate defendants, in the following sectors: consumer products, financial services, information services, media, Internet, non-profit and pharmaceutical. These cases have resulted in over $74 million in judgments or settlements against companies, including over $37.8 million won by the FTC, over $18.3 million won by

state regulators, over $17.8 million won in private class actions and $100,000 won in an individual plaintiff jury award.

The following are recent cases in which significant court rulings were issued or substantial verdicts or settlements were reached. Each case is covered in detail in the *Report*.

DoubleClick Litigation

Class actions were brought against DoubleClick in several jurisdictions, including New York and California. Each case alleged the Internet advertising firm violated its privacy policy by using cookies to identify Web users, tracking the sites they visit, and obtaining other private information about them without consent. In April 2001, a federal court in New York dismissed a class action suit against DoubleClick, ruling that cookies and other technology that tracked users did not violate federal anti-hacking and wiretapping laws. In the California case, however, which was brought under state law, the court has denied DoubleClick's motion to dismiss, allowing the class action to go to trial.

> The court denied DoubleClick's motion to dismiss

Amazon.com Litigation

In this federal class action, plaintiffs alleged Amazon improperly accessed personal customer information in the database of its subsidiary, Alexa Internet. Alexa's Internet-navigation software guides customers to sites that match their online habits. Plaintiffs asserted that Amazon accessed this information - which included names, physical addresses and browsing habits - because it owns Alexa. In April 2001, the federal court in Seattle preliminarily approved a settlement in which Alexa will pay up to $1.9 million to customers whose records are found in the database. Eligible customers may receive up to $40 each. Alexa will also destroy some personally identifiable records in its database. In addition, Alexa agreed to require customers to opt-in to having their data collected before they download the company's software.

Nicholson v. Hooters of Augusta

This state court class action, brought under the federal Telephone Consumer Protection Act (TCPA), resulted in a large jury verdict against a Hooters restaurant. The plaintiff alleged Hooters sent out unsolicited "junk faxes," which featured advertisements and coupons, in violation of the TCPA. The TCPA allows consumers to seek $500 in damages for each unsolicited fax that was sent, and triple damages if the violation was committed "willfully and knowingly." In March 2001, a jury awarded plaintiffs almost $12 million in damages. Hooters of Augusta, which has also filed for bankruptcy due to the judgment, has filed an appeal. This is believed to be the first class action suit under the TCPA to go to trial.

Quintiles Transnational Corp. v. WebMD

This case is an example of a privacy dispute between two companies. Quintiles alleges WebMD breached a contract by suspending delivery of consumer medical data to Quintiles, which uses the information to perform market research for healthcare companies on the effectiveness of their products. WebMD asserted that it stopped delivery of the data to comply with federal and state privacy laws. In March 2001, a federal court in North Carolina rejected WebMD's argument, and issued a preliminary injunction that forced the company to resume transmission of the data. The court stated that even if the data transmissions had violated state privacy laws, the Constitution's Commerce Clause prevents states from regulating the interstate transmission of data. By questioning the constitutionality of state Internet privacy laws, the decision seemingly invites other federal courts to strike down such laws. ■

> WebMD asserted that it stopped the delivery of data to comply with laws

Technology Issues Pose New Challenges in HR Privacy Litigation

Although privacy has long been a concern in the human resources environment, managers are now contending with new and difficult issues that have arisen from increased computer and telecommunication uses in the workplace. So, in addition to conventional HR privacy issues on employee physical surveillance, drug testing and psychological screening, employers must increasingly develop careful policies and be ready to defend against actions involving Internet/e-mail usage and searches of computer data.

***P&AB's** Quarterly Report on Human Resources Privacy Litigation*, available exclusively to members of the CPO Program and the HR Data Consortium, tracks these new legal developments in employee privacy. The *HRL Report* currently covers HR privacy litigation in seven categories: 1) employee computer usage; 2) surveillance of employees; 3) employee searches; 4) release of employee information; 5) drug/alcohol testing; 6) psychological screening and testing; 7) medical screening and testing.

P&AB has compiled information on 30 HR privacy lawsuits. These suits were brought against a total of 23 corporate defendants representing a wide range of industry sectors, including retail, transportation, manufacturing, insurance, media and pharmaceutical. These cases have resulted in over $5.4 million in settlements or judgments against companies.

These cases have resulted in over $5.4 million in settlements or judgments against companies

The following are recent cases where significant court rulings or settlements were reached. Each case is discussed in detail in the *HRL Report*.

EEOC v. Burlington Northern Santa Fe Railroad

In this genetic testing case, the Equal Employment Opportunity Commission (EEOC) challenged Burlington's policy of conducting DNA tests on employees who submit carpal-tunnel syndrome disability claims. The EEOC alleged that Burlington's policy violated employees' privacy rights and discriminated against the disabled. Under a settlement reached in April 2001, Burlington agreed to end its genetic testing policy. The settlement prohibits Burlington from taking any disciplinary action against employees who refused to take genetic tests, and to preserve all records under its control, in case future disputes arise. Burlington also recently settled a similar lawsuit filed by two unions representing railroad employees.

Konop v. Hawaiian Airlines Inc.

The issue in this case is whether an employer can be held liable for accessing a password-protected employee website without permission.The plaintiff is a Hawaiian Airlines employee who operated a website that included statements critical of his employer. He alleged Hawaiian improperly accessed his site in violation of the Electronic Communications Privacy Act (ECPA), which prohibits the unauthorized "interception" of electronic communications. The specific issue before the federal appellate court in San Francisco was whether an interception under ECPA must occur at the same time as the transmission of the communication. Website data is generally stored on a server for a period of time between the initial transmission of the information and the acquisition of that information by its recipients. In January 2001, the appeals court ruled that the case could proceed to trial because ECPA did not require that transmission and interception of a communication be simultaneous. The court stated that ECPA "protects electronic communications from interception when stored to the same extent as when in transit."

Fraser v. Nationwide Mutual Insurance Co.

The court, in this case, was confronted with an issue similar to the one raised in the Konop case, above, but reached a different conclusion. In Fraser, the plaintiff alleged he was illegally fired in retaliation for lodging complaints against Nationwide with state authorities. Specifically, plaintiff claimed Nationwide illegally intercepted his company e-mail in violation of ECPA and state laws. The federal trial court in Philadelphia dismissed the case. The court held that an employer's decision to access employee e-mail in computer storage does not violate any federal or state wiretap laws because those laws are triggered only when the interception occurs "in the course of transmission." Once e-mails are placed in "post-transmission storage," employees have little reason to believe those messages will be private, the court stated.

The plaintiff claimed Nationwide illegally intercepted his company email

In Konop, a federal appeals court reached a conclusion that seemingly contradicts Fraser by holding that electronic communications placed in storage may nonetheless be "intercepted" in violation of ECPA. In contrast, the Fraser court held that wiretap laws only apply while communications are being transmitted. Under Fraser, once electronic communications are placed in storage, employees no longer have any expectation that the communications will remain private. Considering the evolving state of the law in this area, employers that monitor communications systems should notify employees of the practice, and obtain express acknowledgment from employees that they are aware their communications may be monitored.

New PLI Survey Studies Consumer Trust

New findings from Privacy Leadership Iniative (PLI) offer fresh insights in identifying the elements that would enhance consumer trust in using web services based on their personal information.

Working with Harris Interactive in an on-going 18-month study, PLI – an association of 15 leading companies and industry associations – set out to track changes and trends in consumer attitudes, behaviors, experiences and expectations about how business collects and uses consumer information off and online.

In the first two waves of questionnaires, the PLI study confirmed major findings of leading privacy studies over the past decade. For example, their findings include: consumer nervousness about providing companies with what are seen as sensitive personal information elements; high levels of distrust by consumers of either business or government's current readiness or ability to protect consumer's personal data; and increasing privacy assertiveness by majorities of consumers in their relations with companies.

But the PLI study also found that businesses can earn greater consumer trust by posting prominent privacy statements and seals on their websites. Familiarity with brand also encourages consumer trust. Even though consumers tend to trust the offline companies they do business with more than online ones, the PLI study found that well-known dot.coms fare just as well in fostering consumer confidence.

Consumers tend to trust the offline companies they do business with

Among the major findings from the first two waves of the PLI study:

Providing Information Online

- 95% of online users said they were willing to provide websites with basic information such as name, postal address or e-mail address.
- However, respondents were hesitant to provide more sensitive information, such as their income or assets (56%) or Social Security numbers (52%).
- Overall, online users expressed greater confidence in the transmission and use of data using traditional mediums, like the mail (95%) or telephone (80%) versus e-mail (65%) or Internet (60%).

Concerns Online

- The top concern related to use and collection of personal data by online users was uneasiness about information being shared or sold (76%) or that they would receive unwanted advertisements (75%).
- 46% of consumers do not feel that the benefits of using the Internet outweigh the concerns they have.

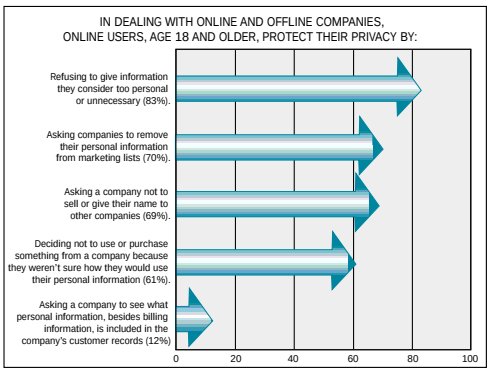
Public Trust in Business and Government

- The public trusts business slightly more than government to protect their personal information and establish effective privacy standards. On a scale of 1 to 10, with 10 being "trust completely," online users rate business a 4.5 while they rate government a 4.1.
- Almost all online users (83-91%) feel it is important to see privacy statements on websites of financial service companies, medical product and service companies, websites for traditional brand name products, new companies that sell only over the Internet and on personal websites.
- Despite a lack of trust in business, nearly half (45%) of Internet users feel websites are doing a "better job" of providing privacy notices and informing visitors of how their personal information may be used.
- While the public views individuals, business and government as sharing responsibility for protecting an individual's personal information, respondents saw individual consumers as having the most responsibility. On a scale of 1 to 10, with 10 meaning "completely responsible," individual consumers received an average of 7.7, compared to 7.2 for business and 6.9 for government.

Privacy Assertive Behavior

In dealing with online and offline companies, online users, age 18 and older, protect their privacy by:

- Refusing to give information they consider too personal or unnecessary (83%).
- Asking companies to remove their personal information from marketing lists (70%).
- Asking a company not to sell or give their name to other companies (69%).
- Deciding not to use or purchase something from a company because they weren't sure how they would use their personal information (61%).
- Asking a company to see what personal information, besides billing information, is included in the company's customer records (12%).



Zoom-in on graph for viewing.

- Few adults, except those who are heavy online users, are even aware of or take advantage of privacy protection tools or technology. Only 10% have bought or installed software on their computer that shields their personal information or allows them to purchase or surf anonymously.

These PLI survey findings are a valuable addition to the survey findings database on privacy, and to the continued study of consumer trust and business practices.

The executive summaries of Waves I and II can be found at:

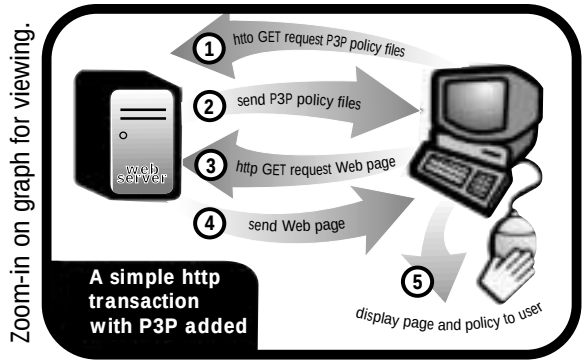
www.understandingprivacy.org/content/library/research.cfm. ■

P3P Debuts – And Stirs Debate

Debates between advocates of privacy legislation and those favoring industry self-regulation began a new chapter with the World Wide Web Consortium's (W3C) near completion of their Platform for Privacy Preferences (P3P).

P3P, designed to give Internet users more control over collection of their personal data and how it will be subsequently used, has been in the works for three years. Users are initially instructed to answer a list of multiple-choice questions about their privacy preferences, choosing the specific attributes of their personal information that they are willing to divulge and those that they wish to keep hidden.

The P3P program will then compare those individual preferences with the privacy policy of the website they wish to enter. If the website's privacy policy is compliant with the individual's preferences, access to the site will be granted. If a discrepancy is found, the program will either alert the user to the specific discrepancy and ask if they are willing to proceed or block access to the site altogether.



Copyright © 1994-2001 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. http://www.w3.org/P3P/brochure.html

According to Daniel Weitzner, a speaker at ***P&AB's*** CPO Washington Briefing and Peer Workshop, all that remains is a final go-ahead from the W3C members. Weitzner expresses confidence in P3P's current configuration, but admits that some changes might be needed after P3P is up and running.

Supporters' Stance

Supporters of P3P say that this new technology addresses consumer's privacy concerns by giving them more control over how others gain access to and use their personal information. P3P will also create a common privacy language for every user and site operator on the web to eliminate the kind of confusion that many consumers expressed about the complicated language used in the recent financial opt-out privacy notices.

Over the past three years, software venders, privacy advocates and commercial users, including the Center for Democracy and Technology, America Online/ Netscape, IBM and Microsoft, have participated in the P3P design effort.

Microsoft's Internet Explorer 6 (IE6) is still in beta testing, but contains all the privacy features that will be available when it is officially released. Additionally, it will be the first browser to support P3P. IE6's implementation of P3P has advertising networks scrambling to ensure their cookie compatibility. The default setting on P3P will allow "first-party" cookies to be set (i.e. the browser will accept a Lycos cookie on a Lycos site), but "third-party" cookies (those placed on a site by a third party) that lack an opt-out option will be automatically blocked.

The Critics

Despite the large number of supporters and the seemingly greater amount of user control over personally identifiable information, P3P has set off a chorus of critics. Many privacy advocacy groups say that the technology is too complex and confusing and it might actually make it more difficult for users to control their privacy.

Browsers will have to negotiate between user privacy standards and site privacy policies every time a user attempts to enter a website. This forces users to make decisions about their personal data for all sites they visit, including those that do not require disclosure of any personal information. This extra burden may make web surfing difficult and time-consuming. Critics worry that these frustrations will cause the majority of users to select the lowest P3P privacy setting.

The negotiating process is based on the specific privacy features laid out in a website's privacy policy; however, the technology is not capable of ensuring the policy's enforcement. Additionally, a website that has strong privacy standards, but does not support P3P might be blocked.

Proponents of stronger privacy laws argue that P3P is just a way of delaying legislation. The need for specific privacy criteria is being overshadowed by a program that is perceived as pro-privacy, but lacks any uniform standard for Internet transactions that could be established by privacy legislation.

In addition to the privacy advocates, some in the business and financial communities are worried about possible disruptions, especially for banks. Online banking services regularly depend on the third-party cookies that risk blockage on the P3P default setting. These disruptions could affect users' ability to make electronic

payments and banks' ability to sell insurance and mutual funds as an intermediary for other companies.

Despite the pros and cons brought up by both the supporters and opponents of P3P, many in the business and consumer community believe that the P3P program, complimented by appropriate "framework" online privacy legislation, would be a valuable step forward on an issue that has no simple or singular solution. ■

Reports Assess Costs of Privacy to Industry

In 2001, several major research reports were published that attempt to assess the direct and indirect costs of privacy to industry. The following are summaries of three reports that explore the costs of implementing privacy protections in three industry sectors – distance shopping, financial services and the Internet.

The Impact of Data Restrictions on Consumer Distance Shopping
Michael A. Turner, Executive Director
Information Services Executive Council

This report estimated the cost of opt-in data restrictions on two segments of the distance shopping industry – catalog and Internet apparel retailers. The study concludes that restrictions prohibiting the use of routine data would severely limit the ability of catalog and Internet apparel retailers to reach the right consumers, substantially increasing their costs.

According to this study, opt-in restrictions would impose a $1 billion "information tax" on consumers, which would result from retailers' increased costs of 3.5 to 11%. This "tax" would disproportionately impact inner city and rural consumers, who depend on distance shopping for their apparel needs the most. The additional costs would also result in less choice for consumers because some retailers will be forced to leave the market while other new companies would not enter at all. Finally, the study concludes that if consumers are required to give consent before a company can use their information, small and new companies would be harmed because consumers are more likely to give consent to firms with significant and favorable name recognition.

> Opt-in restrictions would impose a $1 billion "information tax" on consumers

This study was conducted by the Information Services Executive Council, an industry segment group of The Direct Marketing Association, and sponsored by the Privacy Leadership Initiative. A copy of the full report is available online at www.the-dma.org/isec.

Customer Benefits from Current Information Sharing by Financial Services Companies
Ernst & Young LLP

While focusing on the benefits of information sharing in the financial services industry, this report also details specific compliance costs of implementing the Gramm-Leach-Bliley Act (GLB). GLB - which took effect July 1, 2001 - requires financial institutions to

provide customers the right to opt-out of the sharing of nonpublic personal information with certain third parties, and requires that companies disclose their information sharing practices with affiliates to their customers.

The study concludes that GLB imposes a "high compliance burden" on financial services providers. Specifically, GLB requires financial firms to assess their privacy practices to identify information shared with affiliates or third parties, modify databases and forms to separate shared information and identify customers opting-out, train customer service personnel and provide disclosure statements to customers describing company privacy practices.

The report includes a survey of companies in the Financial Services Roundtable (FSR), a membership organization representing 100 of the largest banking, insurance and securities firms. The majority of FSR companies surveyed said GLB would be "difficult to implement." The study estimates that the costs of implementing GLB just for FSR members are over $400 million, and that overall GLB implementation costs will be much higher. Over half the surveyed companies indicated that 100% of these costs would be passed on to their customers in the form of higher fees, commissions, interest rates and premiums.

100% of costs would be passed on to consumers

Ernst & Young LLP conducted this study for the FSR. To download a copy of the full report, go to www.fsround.org/isuspprs.html#FSRlogo.

An Assessment of the Costs of Proposed Online Privacy Legislation
Robert W. Hahn, Director
AEI-Brookings Joint Center for Regulatory Studies

This study estimates the direct costs of current online privacy legislative proposals to data-collecting websites. Based on 17 estimates from firms in ten states and using multiple technologies, the study assumes $100,000 as the average cost to make websites compliant and to create tracking databases that verify compliance. The study also assumes that the proposed laws could affect as many as 3.6 million websites that collect personal information.

Proposed laws could affect as many as 3.6 million websites

Based on these assumptions, the study estimates that the cost of online privacy legislation would range from $9 billion to $36 billion. The study concludes that further regulation of online privacy is premature because the direct costs of compliance could be substantial, the benefits of such regulation are uncertain and the market continues to respond to consumer concerns about online privacy.

Peter P. Swire, law professor at Ohio State University and Chief Counselor for Privacy in the Clinton Administration, issued a reply criticizing this study, stating there are "serious analytic flaws in the conclusions." According to Swire, the study overstates the costs of legislation because it fails to account for expenses the Internet industry has already incurred for privacy protections it voluntarily put into place. Swire asserts it also fails to distinguish between compliance costs for large and small sites, estimates too many sites, uses unrealistically expensive standards for each site, and assumes that all compliance will be customized.

This study was sponsored by the Association for Competitive Technology, whose membership includes industry leaders and emerging companies in computer software, hardware, consulting and the Internet. A copy of the full report is available online at www.actonline.org/issues/privacystudy.asp. Professor Swire's response to this study is available at www.osu.edu/units/law/swire.htm. ■

Two New Books on Business Privacy

Two recently published books add useful entries to the growing body of literature on privacy and business, and how the consumer-business relationship has been changed by the growth of the Internet. Both works are aimed at businesses attempting to cope in a world where privacy can be both a liability and an opportunity. Their approaches differ, but both may provide valuable additions to the library of the privacy practitioner working in this complex field.

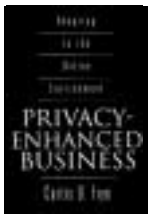
Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan by Michael Erbschloe and John Vacca.
McGraw-Hill, New York, 2001.

Net Privacy by Erbschloe and Vacca provides a concrete series of steps business managers need to take to create and implement a plan to deal with privacy issues. In Chapter One, the authors, who are writers and information technology consultants, argue that it is crucial for business, government and nonprofit organizations to understand the nature and dynamics of the consumer privacy issue. Managers need to know that all organizations are vulnerable to privacy issues in their personal information collection and uses, where the threats are and how to deal with them. In Chapters Two and Three, case studies of privacy crises and how they were handled are

presented. They also provide a general background on privacy law and regulation on the domestic and international levels.

The heart of the book is Erbschloe and Vacca's discussion of the steps businesses should take to make privacy not just an idea, but a concrete plan of action for the company. Before a privacy policy can be developed, let alone implemented, the corporation needs to establish a privacy philosophy and create a privacy task force. Other steps include conducting a privacy audit, evaluating technology, examining Internet supply chains and ensuring data security. The authors also include chapters on desktop and laptop security and telecommuting. There is a handy glossary.

Privacy-Enhanced Business: Adapting to the Online Environment by Curtis D. Frye. Quorum Books, Westport, Connecticut, 2001.



Frye's *Privacy-Enhanced Business* provides a rundown of recent legal and technological developments privacy professionals will find useful. Frye is Principal of Technology & Society, LLC, an electronic commerce and policy analysis firm in Portland, Oregon.

Chapter One looks at the Internet and the way privacy concerns have "poisoned the well." Chapters Two, Three and Four take a snapshot of the legal history of privacy, including Gramm-Leach-Bliley and the EU Directive. Chapter Five examines the value of information in an online economy, how the Internet creates virtual communities and how businesses should handle sensitive information.

In later chapters, Frye discusses forms of online advertising, user-tracking technologies, such as cookies and privacy-enhancing technologies, such as P3P and infomediaries. Frye also includes a brief chapter laying out future privacy-related legislative scenarios. Two appendices contain the full text of the EU Directive and an EU Working Paper on the use of contracts to ensure the security of personally identifiable information.

Both of these books deserve a place on the bookshelves of privacy practitioners. ■

Special permission of Harley Schwadron

Visit us on the web at www.pandab.org/newsletter to subscribe and to learn about our Projects and National Conference.