PRIVACY & AMERICAN BUSINESS
A Comprehensive Report and Information Service

ELECTRONIC NEWSLETTER

Volume 12 • Number 3 March 2005

Privacy Initiatives in the States

It is still relatively early in the legislative year, leaving time for proposed bills to be enacted or to fail. Even so, some state privacy laws have already been enacted in 2005. These enacted laws were proposed in 2004 and carried momentum into this year, or were highly popular and faced little opposition. As of April 1, 2005, the following bills have been approved by their state legislatures:

ID Theft

On March 24, Governor Mark Warner signed into law House Bill 2059. The bill criminalizes the malicious use of a credit card scanner, and creates a separate offense for the sharing of such captured information.

On March 11, 2005, the Governor of Utah signed into law Senate Bill 118, which expands the definition of identity fraud and identity theft crimes to include the fraudulent use of personal information of deceased individuals.

In February, the Governor of Arkansas signed into law House Bill 1354, which clarifies that financial identity fraud pertains to the use of identifying information to open or create a financial account or resource.

Security Breach

On March 30, 2005, a security breach notification bill passed the Arkansas House and Senate (Senate Bill 1167). The bill, sent to the Governor on March 31, would require consumer notification of any actual or potential unauthorized disclosure of the consumer's personal information.

On March 29, Georgia Senate Bill 230 passed out of the House, after passing the Senate 52-0. The bill would require consumer reporting agencies to notify consumers of a security breach. It is awaiting the governor's action.

Spyware

On March 17, 2005, the Governor of Utah signed House Bill 104, which amends Utah's existing anti-spyware law to address constitutionality concerns.

Continued on page 3

P&AB's Dr. Alan Westin Receives IAPP's Privacy Leadership Award.

Harriet Pearson, CPO, IBM and Dr. Alan Westin, President & Publisher, *P&AB*

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. info@pandab.org

PRIVACY & AMERICAN BUSINESS
A Comprehensive Report and Information Service

Privacy & American Business (ISSN #1070-0536), an activity of the Center for Social & Legal Research, is published monthly from Two University Plaza, Suite 414, Hackensack, N.J. 07601. Phone 201-996-1154, FAX 201-9961883, email: ctrslr@aol.com, Website: www.pandab.org and www.PrivacyExchange.org. Subscriptions are $295 for 12 issues; additional subscriptions within a subscriber organization are $50. Academic and library subscriptions are $120 for 12 issues. Special rates are available to cooperating organizations.

Hearing from Nostradamus

Earlier this month, Alan Westin was honored by IAPP and received the 2005 Privacy Leadership Award at their Privacy Summit in Washington, D.C. Dr. Westin's presentation of his predictions for the privacy world in the next few years was one of the features of his appearance there, and will be expanded into an *In Depth* item in April's issue of ***P&AB***.

From ID Theft to Japan Data Protection

You'll find in this issue a discussion of some of the really hot topics heading the state legislators' agendas so far in 2005 (see page 1). We would like to thank State Net for their help. ***P&AB's***, regular feature, *ID Theft Update*, takes a look at the latest incidents involving consumers and the latest legislative highlights trying to curb this morphing threat affecting companies and consumers (see page 7). You'll get a peek at the most recent surveys on ID theft, as well as what consumers are thinking and how they are responding to this crime. Moving to the global scene, ***P&AB*** welcomes Japan as it officially joins the community of nations with omnibus data protection laws.

Mark Your Calendar for P&AB's Next Tele/Web Conference

Following our very successful Tele/Web Conference on the Privacy Year in Review, we have set May 10, 2005, 2:00 PM EST for ***P&AB's*** next important Tele/Web effort. We're focusing on outsourcing and its more contentious sister, offshoring – a high profile topic that has captured the attention of business, governments and the public.

We've asked one of our members, a recognized hands-on expert on the topic's many facets, to bring to the table *Privacy, Outsourcing and Offshoring: What You Need to Know*. Barbara Lawler, CPO, Hewlett Packard, who has both a national and global perspective, will lead the session. You'll have an opportunity to ask questions during the Tele/Web Conference if you participate online.

We hope you'll join us and bring your organization's privacy, compliance, legal, marketing, HR, government relations and others with you. For special group rates, contact Olga Garey at (201) 996-1154 or info@pandab.org. And, we'll help you with your CLE credits.

Planning Ahead

We are planning more of these events, so if you have a privacy or privacy-related subject you'd like to have explored by the experts, let me know.

If You've Missed...

If you missed ***P&AB's*** Privacy Year in Review, Projections and Trends 2005, log in ANYTIME and attend virtually! The full audio and slide deck presentation are available. If you missed it, you'll want to hear Alan Westin and Bob Belair as they offer listeners the most on-target analysis of the privacy scene in the states, in the courts, at the federal level, and in public opinion. To sign up, visit www.pandab.org to download the registration form and fax it to Olga Garey (201) 996-0488 to receive your log-in information.

Insurance Industry Privacy & Security

P&AB is a co-sponsor of an important and wide-ranging conference hosted by the American Conference Institute slated for June 27-28, 2005 in New York City. "The National Forum on Privacy & Security in the Insurance Industry" will include top-drawer speakers and panelists who will focus on the latest privacy and security issues and developments in insurance. To receive your $200 discount, download the registration form available at www.pandab.org. For more information about the conference, visit www.americanconference.com/insprivacy.

Three New Reports in 2005

The first of ***P&AB's*** 2005 special reports are already in the hands of our members – ***P&AB's*** *Consumer Privacy Survey Trend Report*, the *Global Privacy Trend Report* and *Privacy Legislation in the States*.

P&AB's Special Reports are written by experts, including Alan Westin, who have their finger on the privacy pulse of the U.S. and the globe. Successful CPOs across all industries refer to our materials for the most up-to-date information and deep analysis of the issues. In a few weeks, these will be available to non-members, so those interested should place their orders today! Visit www.pandab.org, or contact Olga Garey at info@pandab.org for more information about receiving the Reports or about becoming a ***P&AB*** Member.

Lorrie Sherwood
Executive Editor

Spam

On February 1, 2005, Ohio Governor Bob Taft signed into law anti-spam legislation that creates criminal and civil penalties for transmitting multiple commercial electronic messages (House Bill 383).

Ohio's new anti-spam law imposes criminal and civil penalties

Internet Content

On March 21, 2005, the Governor of Utah signed into law House Bill 260, which requires the state to create an "adult content registry." The law provides that "upon request by a consumer, a service provider shall filter content to prevent the transmission of material harmful to minors." Further, "upon request by the consumer, a service provider may not transmit material from a content provider site listed on the adult content registry." The law takes effect on January 1, 2006.

Telecommunications

In February, the Governor of South Dakota signed into law Senate Bill 20, which limits disclosure of wireless phone numbers. The new law states that no provider of a mobile telecommunications service, or their affiliates, may publish a wireless directory or include a subscriber's wireless telephone number in a wireless directory assistance service database, without prior authorization from the consumer.

Faxes

Colorado House Bill 1059 passed both the House and the Senate unanimously. The bill would limit exemptions currently existing to the state's law against sending unsolicited faxes.

Social Security Numbers

On March 23, Governor Warner of Virginia signed into law House Bill 2482 that limits the display and use of Social Security numbers.

In January, New Jersey's governor signed into law Assembly Bill 1205, which prohibits institutions of higher education from displaying students' Social Security numbers by posting or public listing of grades, on class rosters or other lists provided to teachers, on student identification cards, in student directories, or similar listings.

In February, Governor Mike Huckabee of Arkansas signed into law House Bill 1117, which removes the Social Security number from the information to be provided on a petition for a protective order.

STATES LEGISLATION TO CURB IDENTITY THEFT

State legislators, in an effort to curb ID theft in their own states, are regulating consumer reporting agencies (CRAs), and giving consumers more tools to access and control their personal information. Popular proposals in 2005 include giving consumers the ability to place a "security freeze" on their credit report and requiring CRAs to provide free credit reports.

Pending State Legislation: Credit Reports

New York Assembly Bill 2515 would require CRAs to attempt to verify information by "proper, fair and reasonable means" in their reports. Another bill, New York Assembly Bill 3004, would require CRAs to pay a $.50 fee to the subject of a credit inquiry whenever they provide a consumer report or investigative consumer report.

Utah House Bill 100 – the Utah Consumer Credit Reporting Act – would require a CRA to notify the consumer within five business days after furnishing their credit report. Notification includes the name of the person who requested the consumer's credit report, and the date on which the credit report was furnished.

South Carolina House Bill 3508 would enact "The South Carolina Fair Credit Reporting Act." The law would forbid granting access to a credit report, except as permitted by federal law. The law permits a right to sue, and offers actual and punitive damages.

Rhode Island has a bill pending (House Bill 5180) which would prohibit CRAs from using the number of credit checks ordered on any person as an indicator of their credit.

A bill pending in Ohio (House Bill 28) would prohibit CRAs and anyone granting credit from discriminating on the basis of sexual orientation.

Pending State Legislation: Security Freeze

By mid-2005, California, Texas, Louisiana and Vermont will all have laws in force allowing consumers to restrict access to their credit reports. Federal law provides for fraud alerts, but does not give consumers the right to place a "security freeze" on their credit report. Therefore, new state laws that allow security freezes will not be preempted.

By mid-2005, California, Texas, Louisiana and Vermont will all have laws in force allowing consumers to restrict access to their credit reports

A number of bills allowing consumers to "freeze" access to their reports are pending in the states (see box below).

Pending bills allowing consumers to instruct credit reporting agencies not to allow access to their reports:

- Colorado Senate Bill 137
- Connecticut Senate Bill 950, Senate Bill 650
- Hawaii Senate Bill 764
- Illinois Senate Bill 1892, House Bill 1058
- Indiana Senate Bill 178
- Maine Senate Bill 190
- Maryland House Bill 1569
- New York Assembly Bill 2785
- Oregon House Bill 2412
- Washington Senate Bill 5418 and House Bill 1468

Consumers Receive A Free Credit Report

Relatively few states have proposed laws requiring CRAs to give consumers a free credit report. The reason for this is any proposed state legislation may be preempted by the FACT Act. But, some states are taking the plunge anyway:

- Iowa Senate Bill 1038 would require CRAs to give consumers one free credit report every year. The bill would permit the consumer to sue for actual damages, attorney fees and court costs.
- Connecticut Senate Bill 174 would require CRAs to give state residents one copy of their report, free of charge, at regular intervals.
- New York Senate Bill 320 would give consumers the right to one free copy of their credit report.

SECURITY BREACH NOTIFICATION LEGISLATION

In the wake of news stories about the loss of consumer information by data brokers and others, a number of state legislators from both parties have proposed laws similar to one already in place in California. These laws would require a business to notify a consumer if there is reason to believe their information may have been illegally accessed by a third party.

In 2003, California enacted the "Security Breach Information Act," which requires businesses that maintain personal information to notify consumers if their data has been disclosed as a result of a security breach.

ChoicePoint originally disclosed its security breach to California residents, as required by law. The incident has led legislators in other states to propose their own version of the California law. Some businesses argue that if a law requires notification, there should be some evidence of identity theft, or consumers will receive too many notices, which they may ignore.

Bills to Watch

- Georgia Senate Bill 230 would require any CRA holding personal information to notify the consumer of a security breach if their data is reasonably believed to have been acquired by an unauthorized person.
- Illinois Senate Bill 1899 would create the Identity Theft Notification Act. The bill would require any agency, person or business that conducts business in Illinois, and owns or licenses personal information about an Illinois resident, to notify the resident that there has been a security breach involving their data.
- New York Assembly Bill 1525 would force banks to disclose certain security breaches involving personally identifiable information.
- Arizona House Bill 2575 would require that, within 48 hours of discovering a theft of personal information, a person or entity must inform all of their customers of the theft and advise them how to guard against unauthorized use of their information.

Other security breach notification laws are pending in Arkansas, Colorado, Idaho, Maryland, Michigan, Minnesota, Missouri, Montana, New Jersey, North Dakota, Oregon, Rhode Island, Tennessee, Texas, Virginia, Washington and West Virginia.

SPAM ON STATE LEGISLATORS' PLATE

For several years, spam has become a significant problem for individuals, businesses, and Internet service providers. Federal legislators addressed the problem with the CAN-SPAM

State legislators have continued proposing and enacting anti-spam laws

Act. Effective in 2004, the law bans false headers and subject lines, and requires recipients be given an opportunity to opt out.

The CAN SPAM Act preempts state spam laws regulating unsolicited e-mails, but does not preempt state spam laws that forbid falsity or deception in commercial emails; or laws that relate to trespassing, contract or torts, fraud, or general computer crimes.

States Going Beyond CAN SPAM

State legislators have continued proposing and enacting anti-spam laws, even after the passage of the federal CAN SPAM Act. One example is Ohio's anti-spam legislation signed into law on February 1, 2005 by Governor Taft. This law creates criminal and civil penalties for transmitting multiple commercial electronic messages (House Bill 383). The new law, which takes effect 90 days following the governor's signature, makes it illegal to send multiple commercial e-mails "with the intent to deceive or mislead recipients as to the origin of those messages." The law also bans inserting false headers in multiple commercial e-mails, and registering e-mail accounts using a false identity for the purpose of sending mass commercial e-mails.

The Ohio law targets smaller spammers who could receive up to 18 months in prison and fines of up to $25,000. E-mail violations would be considered fourth-degree felonies, the most serious offense, if a sender's volume exceeds 250 during any 24-hour period, 2,500 during any 30-day period, or 25,000 over a year.

Pending Anti-Spam Laws

- For e-mails using false or deceptive headers, Nebraska Legislative Bill 393 would levy a $500 fine, as well as allow for suits for lost profits and attorney's fees.
- New York Assembly Bill 3002 would prohibit the transmission of unauthorized and misleading electronic mail. Bill 227 would require senders of unsolicited commercial e-mail to provide their name, street address and e-mail address.

There are anti-spam bills pending in California (Senate Bill 97); Connecticut (House Bill 5260); Indiana (House Bill 1501); Minnesota (House Bill 243); Mississippi (House Bill 148); and New Jersey (Assembly Bill 419, 3393).

STATES TAKE A BITE OUT OF SPYWARE

"Spyware," and "adware," were hot privacy buzzwords in 2004. While experts agree that spyware is a problem, not everyone agrees on what should be regulated, and, if regulated, how it should be done.

Generally, state spyware bills attempt to define spyware and forbid another person or party to download software onto a user's computer without notice or consent. California and Utah enacted spyware laws in 2004. On March 17, 2005, however, Utah amended its law in response to numerous complaints and a court challenge.

Utah: A Spyware Case in Point

After *1-800 Contacts*, a Utah-based company, alleged that *WhenU* was using spyware to divert customers from its website, Utah became the first state to enact spyware legislation. *WhenU* fought back and filed suit in Utah, alleging that the law was unconstitutional. A Utah judge agreed and issued an injunction in June 2004.

Many other companies, including Amazon, eBay, Google, Yahoo, and Microsoft, also argued that the law was flawed and could ban legitimate communications. In response to these criticisms and concerns about the law's constitutionality, Utah state legislators passed House Bill 104 to amend its existing 2004 law.

California Follows Suit

In September 2004, Governor Schwarzenegger signed the Consumer Protection Against Spyware Act, making California the only other state to enact a spyware law. The California law makes it illegal to, with actual knowledge, or willfully, cause software to be copied onto someone else's computer, to change certain settings, to block the disabling of software, and open certain advertisements. Although the law does provide for an individual's right to sue for damages of $1,000, privacy advocates objected to the bill, saying that standards of proof were too high, and that the law was "unenforceable."

Bills to Watch

- Michigan Senate Bill 54 would make it illegal to install, or attempt to install, spyware on another person's computer. The law would define spyware as a computer program that deceptively monitors, collects, copies, or transfers information from a computer.

- New York Assembly Bill 2682 would amend the penal code to criminalize the unlawful dissemination of spyware. The law refers to spyware as an "executable computer program, including but not limited to a keylogging program, that employs a computer user's Internet connection without the computer user's knowledge or explicit authorization and such computer program gathers and transmits personal information or data of a computer user."

> NY's Bill 2682 would amend the penal code to criminalize the unlawful dissemination of spyware

- Tennessee Senate Bill 2069 would prohibit installation of spyware without consent. The bill defines spyware as software with a "context based triggering mechanism."
- Nebraska Legislative Bill 316 would make it illegal to install software onto someone else's computer to modify their settings or collect personal information through intentionally deceptive means.

Spyware laws are also pending in Alaska, Alabama, Arizona, Arkansas, California, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Maryland, Massachusetts, New Hampshire, Texas, Oregon, Utah, Pennsylvania, Rhode Island, Virginia and Washington. ■

With John Haley

P&AB's** State Privacy Legislation Report: Trends* and Issues examines state legislative activities across the privacy spectrum. This unique report is made available in advance to ***P&AB Grantors, PLG Members and Grantors. Non-members may place their order May 16, 2005.

Mark Your Calendar!

P&AB's Eleventh Annual National Conference is set for December 6-7, 2005 in Washington, D.C. This landmark event has been the place for cutting edge analysis of privacy trends and developments, high calibre speakers and resources, and timeliness.

Save the date and check www.pandab.org for information.

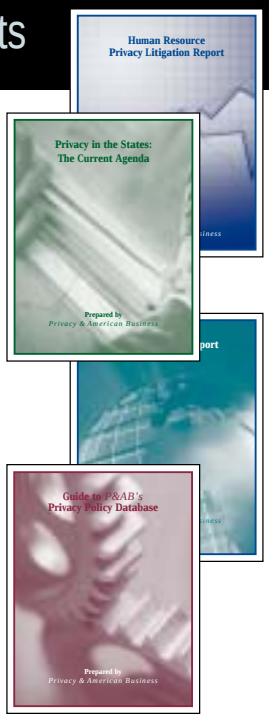
Details will be posted soon.

P&AB's Special Privacy Reports

Every expert privacy practitioner has a copy of *P&AB's* Special Privacy Reports. Up-to-date, with the most extensive analysis of privacy trends and developments, these reports can be found nowhere else:

- Consumer Privacy Litigation Annual Round Up
- Privacy Legislation in the States
- The Global Privacy Trend Report
- HR Privacy Resource Guide
- CPO Job Description and Evaluation Criteria: What Management Should Know
- Consumer Privacy Surveys Report
- Guide to *P&AB's* Privacy Policy Database

Visit www.pandab.org to download the tables of contents or to find out how you can receive your copy today!



P&AB Identity Theft Update

***P&AB** selects valuable news reports on ID theft from print and online publications, summarizing them from the content and perspectives of the publications reporting them.*

New Poll Shows ID Theft Still On The Rise

Since ChoicePoint revealed the theft of personal records by individuals posing as businesses, there has been heightened awareness and increased public concern over identity theft and the adequacy of steps businesses have taken to protect their customers. An ABC News/ Washington Post poll on identity theft revealed that 84% of the public do not believe that businesses are doing enough to protect their personal information. Almost two-thirds (62%) of the public believe these security measures of data broker firms are not sufficient. And, three out of four Americans (76%) are fearful that they will be victims of identity theft in the future.

> 76% of the public fear they will be victims of ID theft in the future

"Identity Theft," ABC News/ Washington Post Poll. March 15, 2005.

BUSINESS INITIATIVES

New Consumer Tools

Public outcry over identity theft has prompted some companies to adopt new authentication methods for the safety of their customers. E*trade Financial's "token-based" system, for example, provides two layers of password protection. This system uses one password that remains static, in addition to one that constantly changes for enhanced protection. AOL has adopted token technology for its subscribers, while also providing a firewall and other protection against viruses and spyware.

Another major player in the online arena, Ebay, has implemented a "Web Caller-ID," a downloadable plug-in that verifies the authenticity of a website.

Equifax's new toolbar, downloadable from their website, determines the level of safety on websites. Powered by Earthlink, the toolbar alerts customers to phishing scams and enables them to verify the authenticity of websites. Equifax has also included ScamBlocker, a product also developed by Earthlink, to alert customers to known phisher sites.

"Companies scramble to bolster online security," Computerworld New Zealand March 8, 2005.
http://computerworld.co.nz/news.nsf/0/BFF81EFB9EAA4145CC256FBD00664EC7?OpenDocument&pub=Computerworld

Identity Cops Product Tackles ID Theft Before It Happens

Identity Cops, a credit card and credit report monitoring service, has developed PrivacyProBot™. This new technology searches hundreds of databases and reports information that is inaccurate or may lead to identity theft. The subscription-based service offers consumers options to fix problems PrivacyProBot™ may find. For victims of ID theft, Identity Cops also provide "individualized prevention and recovery services for customers with more comprehensive needs." For more information on Identity Cops and PrivacyProBot ™, visit www.identitycops.com.

"Identity Theft Protection Company Unveils the Only Real Prevention Technology Available Today – Credit Card and Credit Report Monitoring is Just the Tip of the Iceberg," eReleases™ March 15, 2005. http://www.ereleases.com.

GOVERNMENT ACTIONS TO CURB ID THEFT

Attorneys General Take Extra Measures

Attorney General Thomas F. Reilly of Massachusetts and Attorney General Rob McKenna of Washington have each taken measures to fight ID theft. Reilly has called attention to limitations of current ID theft laws and has vowed to introduce a plan that would "close a series of jurisdictional loopholes." However, McKenna noted a deficit on ID theft prevention spending and is asking for an additional $3.5 million in the consumer protection division's budget to increase the legal staff and add more assistant attorneys general.

> Attorneys General are beefing up consumer protections against ID Theft

"McKenna seeks millions to fight ID theft," Seattle Post Intelligencer. February 8, 2005.
http://seattlepi.nwsource.com/local/211113_idtheft08.html

"Massachusetts AG seeks tougher identity-theft law," The Boston Globe. February 11, 2005.
http://www.boston.com/business/articles/2005/02/11/massachusetts_ag_seeks_tougher_identity_theft_law/

ID Theft Teams

With Washington now ranked the 10th worst state in the nation for ID theft, Detectives Dave Startup and Jesse Regalado have been assigned to investigate ID theft and fraud cases in the state. So far, the two have "turned roughly 15 cases over to prosecutors in at least six counties, where charges are now pending." In addition, they have 13 open cases and are conducting educational seminars, particularly in areas where methamphetamine use is prevalent. The use of methamphetamine has been linked to a high number of ID theft incidents.

"New ID-theft team has heavy workload," The Seattle Times. February 10, 2005.

http://seattletimes.nwsource.com/html/localnews/2002175946_idtheft10m.html

ID Theft Task Force

Nevada, holding the Number Two spot for highest number of ID theft victims in the U.S., has put together a law enforcement task force to reduce identity theft. Undercover police and federal agents are examining holes in computer systems that may allow identity thieves to access personal information. SWIFT (the Southwestern Identity Theft and Fraud Task Force) has indicted 64 criminals in the last ten months; six have been convicted.

"New Task Force Targets ID Theft Criminals," KLAS-TV (Las Vegas, Nevada). February 11, 2005.

http://www.klastv.com/Global/story.asp?S=2936389&nav=168YWHd8

May I Have Your License, Registration and Fingerprint?

Arizona ranks Number One in the nation for the highest number of ID theft victims. To change this ranking, Phoenix Sheriff Joe Arpaio is asking motorists to voluntarily submit a fingerprint when pulled over for a traffic stop. Collection of these fingerprints has already begun. Later, these prints will be run against a database system to see if a false identity was used. Motorists are reminded that there is no penalty for those who do not want to give their fingerprint. A similar program in Green Bay, Wisconsin was suspended after much public criticism.

> Arizona is ranked Number 1 with the highest number of ID theft victims in the U.S.

"Arpaio wants drivers' thumbprints; some say he shouldn't ask," The Arizona Republic. February 4, 2005.

http://azcentral.com/arizonarepublic/news/articles/0204fingerprint04.html#

CONSUMER GROUPS WEIGH IN

Privacy Groups Up In Arms Over ID Theft Insurance

For the past five years, insurance companies have been offering ID theft insurance to protect individuals against losses up to $25,000. Because of heightened awareness about identity theft and fraud, the sale of this insurance has climbed. Linda Foley of the Identity Theft Resource Center stated, "We're not fond of a lot of [identity theft insurance] products being sold today based on the hysteria caused by identity theft. We call them profiteers. There's a lot of free help out there."

"Privacy groups not thrilled with ID-theft insurers," Atlanta Journal Constitution. March 12, 2005.

http://www.ajc.com/business/content/business/0305/12insure.html

IDENTITY THEFT AND DATA SECURITY BREACHES

AOL Update

Last June, one of the largest and most provocative identity theft stories hit the newsstands when former AOL employee Jason Smathers, 24, was arrested for stealing and selling customer information obtained while he was employed there. In early February, Smathers pled guilty to these charges via a plea agreement. Sentencing will be in May when he will face between 18 months and two years in prison and a fine of several hundred dollars to AOL.

"Guilty plea for AOL data theft," Out-Law News. February 7, 2005.

http://www.out-law.com/php/page.php?page_id=guilty-pleaforaol107785590&area=news

Warnings: Your Information Has Been Exposed

Science Applications International Corp. (SAIC), a government defense contractor, warned 45,000 employees of a computer theft. These stolen computers hold personal information of current and past employees and shareholders. No incident of identity theft has been reported so far and there is no evidence to suggest that theft of personal information was the intended crime. The notification of the employees was taken as a precautionary measure.

"San Diego defense contractor warns employees following computer theft," San Jose Mercury News. February 4, 2005.

http://www.mercurynews.com/mld/mercurynews/news/breaking_news/1-8-9669.htm

Ryan Pirozzi in Edina, Minnesota was mistakenly sent 86 account statements containing the personal information of 73 individuals with Wachovia accounts. The bank quickly investigated and found that one clerk had mistakenly entered Pirozzi's address that linked it with other customers. Most of the accounts were already closed by the time the letters reached Pirozzi. Addresses were corrected when they were returned to the bank.

"Your Statements Went Where?" The Washington Post. February 6, 2005.

http://www.washingtonpost.com/wp-dyn/articles/A439-2005Feb5.html

Bank of America (BofA) notified the U.S. Department of Defense and the General Services Administration in late February that it had lost several tapes containing customer information. In early March 2005, BofA reported the loss of tapes holding the information of 1.2 million federal employees, including U.S. Senators. The incident occurred late last year when records were being moved to a storage facility. The bank may move towards a "network-based disk-to-disk backup system" to eliminate the threat of theft or loss of tapes and physical records.

"Data Snafus Spur IT Action: Bank Mishap Prompts Call for Network Backup," Computerworld. March 7, 2005.

http://www.computerworld.com/governmenttopics/government/legislation/story/0,10801,100220,00.html

Retail Ventures Inc. reported the theft of at least 103 customers' transaction and credit information at the DSW Shoe Warehouse store. It is believed that a hacker is responsible. An investigation should be wrapped up in the next few weeks.

"DSW Shoe Warehouse Reports Customer Data Theft," Reuters via WashPost. March 8, 2005.

http://www.washingtonpost.com/wp-dyn/articles/A17831-2005Mar8.html

Approximately 1,700 blank Nevada licenses were stolen from the Department of Motor Vehicles when a truck crashed through one of its walls. Thieves also took a digital license camera, a computer and printer that could be used to create fake licenses. Authorities worry that if thieves were to create licenses, they could be used in conjunction with stolen records or documents to carry out ID theft. Although they could create a license virtually identical to a real Nevada license, there would be no record of the license in the Nevada Department of Motor Vehicles. ■

"Authorities warn of consequences of DMV break-in," Las Vegas Review-Journal. March 9, 2005.

http://www.reviewjournal.com/lvrj_home/2005/Mar-09-Wed-2005/news/26027160.htm

With Christie Lawrence

ID Theft in the States

- As in Florida, Illinois' governor is calling for stronger state protections for identity theft. In case of personal data theft, both out-of-state and in-state businesses must notify Illinois residents. Minnesota Senator Satveer Chaudhary and Representative Jim Davnie introduced a similar notification law. Other security breach laws are expected to be introduced in Colorado, Maryland, Missouri, North Dakota, Tennessee and Washington.
- The Indiana Supreme Court ruled that court records including personal information, such as a Social Security number, must be printed on light green paper to protect the paperwork from being viewed by third parties and the information from being stolen or used for illegal purposes. The green paper would be kept in a manila folder and removed before giving the file to the person who requested it.
- Massachusetts Attorney General and State Representative Paul Casey filed a bill to toughen identity theft sentences and legislation that would facilitate the apprehension of suspects in a different state.
- Several Michigan laws enacted in early March address ID theft and fraud: companies are banned from denying credit to ID theft victims; and a maximum penalty and fine for identity theft crimes has been set.
- Enacted last month, NJ state colleges and universities ended the use of Social Security numbers as the primary student identifier.
- With legislation to be introduced in the next 60 days, the crime of ID theft will be considered a felony in New Mexico. The bill also includes provisions for an identity theft "passport," to help victims in putting their finances back in order.
- Oklahoma Representative John Nance introduced a bill restricting the use of Social Security numbers by businesses on any document or card designed to be carried in a wallet. His prime concern is health insurance cards.
- Texas AG endorsed SB 122, that would allow the Attorney General's office to request fines against those involved in ID theft. It also requires local law enforcement to write a report of any alleged ID theft.

For a more thorough report and for other state privacy laws, order ***P&AB's*** States Report and Analysis available in the coming weeks. Order your copy today!

PRIVACY & AMERICAN BUSINESS
A Comprehensive Report and Information Service

Privacy, Outsourcing and Offshoring: What You Need to Know

Following our very successful Tele/Web Conference on the Privacy Year in Review, we're getting ready for *P&AB's* next important Tele/Web effort. We're focusing on outsourcing and its more contentious sister, offshoring – a high profile topic that has captured the attention of business, governments and the public.

Attention Attorneys: You may earn CLE credits by participating.

When: May 10, 2005, 2:00PM EST

Who: Barbara Lawler, CPO, Hewlett Packard and Dr. Alan Westin, President & Publisher, ***P&AB***

What: Privacy, Outsourcing and Offshoring: What You Need to Know

☐ Yes, register me for ***P&AB's*** Tele/Web Conference, Privacy, Outsourcing and Offshoring: What You Need to Know!

Company

Contact Name

Title

Address

City | State | ZIP

Phone | Fax

Email

Rates: ☐ *Member Rate: $150 ☐ Non-member Rate: $175

P&AB* PLG Members and Fellows Receive Complementary Registrations. To find out how you can become a **P&AB Member, contact Olga Garey at (201) 996-1154 or visit www.pandab.org.*

Method of Payment:

☐ Enclosed Check ☐ Credit card ☐ Amex ☐ Visa ☐ MasterCard

Credit Card Number | Expiration Date

Signature:

Fax Registration Form to: 201-996-0488

For questions, contact Olga Garey at (201) 996-1154 or info@pandab.org.
A confirmation email will be sent to the email address provided.

If you missed *P&AB's* Privacy Year in Review, Projections and Trends 2005, log in ANYTIME and attend virtually! Visit www.pandab.org, or contact Olga Garey at (201) 996-1154 or info@pandab.org for details.

A New Privacy Era Dawns in Japan

On April 1, 2005, Japan officially joined the community of nations with omnibus data protection laws, as the Personal Information Protection Act (2003) came into full effect. The Act imposes new requirements on businesses in Japan that handle the personal data of more than 5,000 individuals. Among other things, those businesses will now need to:

- Provide consumers with information about the collection and use of their personal data
- Maintain strict standards of data security
- Seek consumer consent for data sharing
- Give consumers access to their personal files and an opportunity to request that errors in those files be corrected.

Also in effect April 1 were some twenty binding, sector-specific guidelines drafted under the Act by various government Ministries and Agencies. Among them are Ministries of Health, Labor and Welfare (MHLW), Internal Affairs and Communications (MIC), Economy, Trade and Industry (METI), and the Financial Services Agency. The 20 guidelines will apply to areas as diverse as healthcare and insurance, DNA testing, credit and finance, electronic communications, broadcast subscriber records, and job applicants' and employees' personal data.

A Sea Change in Japan's Approach to Privacy

The advent of the Act represents a sea change in the Japanese privacy landscape. Until the late 1990s, the Japanese Government was committed to promotion of industry self-regulation (supplemented by Ministry advice and guidance) as the best way to address the issues of personal data protection in the private sector. As recently as 1998, then-Prime Minister Yoshiro Mori and former President Bill Clinton issued a Joint Statement on Electronic Commerce that emphasized continuing industry self-regulation of consumer privacy and data protection issues.

Japan moved away from the self-regulatory model around the turn of the millennium, when the Government began laying the foundation for e-government services and creating measures to foster the growth of Japanese e-commerce. Realizing that success in both areas would require high levels of individual trust in personal data handling, the Government proceeded to establish working groups to discuss ways of strengthening data protection in the Japanese public and private sectors.

These working groups were faced with declining levels of trust among the Japanese people in both business and government generally, and in corresponding levels of their unease with institutional management of personal data specifically. The Japanese media has long focused close attention on incidents involving leakage or mishandling of personal information. Media reports on this topic have contributed to strong public concerns over information privacy. Against this background, in 1999 and 2000, the working groups recommended an omnibus data protection law, which was eventually enacted as the Personal Information Protection Act on May 23, 2003.

Will the Act Increase Consumer Trust in Business?

Almost two years have elapsed since passage of the Act. In that time, consumer concerns over mishandling of personal data have continued to grow. These fears have been fueled by major data leaks and related incidents at high-profile businesses such as Softbank, Disney, Citibank, Lawson Convenience Stores, NTT DoCoMo, Sanyo Shinpan, Family Mart, Cosmo Oil, and many others. The period has also seen growing consumer dissatisfaction – in the form of an apparent increase in suits filed – with traditional remedial measures taken by Japanese businesses following a privacy incident, such as token voluntary payments to affected consumers, and promises to tighten data security.

While data protection laws can sometimes increase public trust in personal data handling within regulated industries, early signs suggest that this will not be an easy sell in Japan. For example, a 2004

nationwide survey of Japanese consumers, sponsored by the Center for Social & Legal Research's (parent organization of ***P&AB***) Japan-U.S. Privacy and Data Protection Program, found that, although awareness of the new Act was high (at 81.9%), six in ten Japanese consumers (61.9%) were not confident that it would lead businesses to "protect consumers' privacy thoroughly." In the face of public skepticism, the new law's impact on consumer trust in corporate personal data handling will depend on the way both businesses and government implement the Act in practice.

Making the Act Work

Making the Act work to increase consumer trust will require a genuine commitment on the part of the Ministries to transparent, meaningful and consistent enforcement. The Act, as written, does not make specific provisions for consumer-initiated privacy complaints nor for redress or compensation in the case of proven legal breaches (as are found in most other omnibus data protection laws). As a result, any long-term failure to enforce will undercut the Act's ability to increase consumer trust and may spark a rise in privacy lawsuits.

As these lawsuits will now be based on violations of a specific data protection law, the potential for substantial damage awards has risen significantly – a fact that has not escaped the notice of major Japanese insurers. Many are now offering data leak packages to their corporate clients. In 2002, a Japanese court awarded three plaintiffs ¥15,000 (approximately $140) each in damages in relation to a leak, even though there was no apparent secondary harm (such as identity theft). Pending cases include claims of up to ¥1 million (approximately $9,330) per plaintiff. Obviously, in future cases involving large numbers of leaked customer files, court-ordered damages could potentially reach into the billions of yen.

Technology Fixes Not Enough

Recent media reports suggest that many Japanese businesses are preparing for the commencement of the Act by strengthening customer data security through installation of hard drive-free terminals, setting up restricted access databases, and implementing new rules and training for staff who handle customer data. While vital for both compliance and trust, improved data security alone will not be enough. To reap the potential benefits of the Act, and to reduce its potential for increased litigation, businesses in Japan must ensure that they also fully address the privacy requirements of the Act – those that address consumer rights to notice, access, correction and refusal to consent to certain types of data use and sharing.

Since the new law also covers employee personal data collection and uses, every company operating in Japan – whether it offers consumer products and services or not – must bring its personnel and human resources records, databases, and data communication systems into compliance with the law and ministry guidelines. Japanese companies will also need to address compliance with the new law in their transborder personal data transfers and their outsourcing operations. Both of these activities are covered by the new law in exactly the same terms as handling personal data within Japan.

There is evidence that businesses in Japan are now beginning to address these requirements. For example, Sumitomo Mitsui Banking Corporation's recently released, law-compliant privacy policy addresses the corporation's purposes for using personal data, a commitment to use fair and secure methods for obtaining and storing such data, and lays out the procedures by which customers can obtain access their personal information. The bank has posted the policy on its Japanese-language website, and has set up a dedicated phone service to handle consumer inquiries about personal information handling and management.

A Challenge and An Opportunity

The commencement of the Personal Information Protection Act represents a significant compliance challenge to businesses in Japan, which have operated in a self-regulatory environment. There is no doubt that it increases every data handler's exposure to legal and associated risks. However, by establishing baseline legal requirements to respect consumer privacy, the Act also affords a significant opportunity for Japanese businesses to rebuild the trusted relationships with consumers necessary for success, both online and off. ■

With Vivian van Gelder and Alan F. Westin

Continued on page 13

ASSISTANCE TO COMPANIES

The Japan Privacy Resource Website

Corporate staffs wishing to follow developments in Japan related to consumer and employee privacy can go to the Center's free website – the **JAPAN PRIVACY RESOURCE (JPR),** already Google's #1 and #2 worldwide website on Japan + privacy. The JPR offers reports and analysis, as well a range of libraries, including laws and regulations, surveys, papers and reports, a Japanese company privacy policy database, and an e-government and privacy resource. Readers can also sign up for our free monthly Japan NewsFlash by sending their name, title, address and e-mail address to admin@privacyexchange.org.

The JPR NewsFlash provides an up-to-date news stream on business, government, consumer and legal developments affecting consumer-business, citizen-government and employee-employer privacy relationships in Japan.

The Japan Privacy Center

Helping companies in Japan to define and apply good privacy policies will be a service of a new Tokyo-based consultancy, the **JAPAN PRIVACY CENTER (JPC),** led by business strategist Jun Sofue and Dr. Alan Westin. The JPC includes privacy risk assessment and privacy-law-compliance services but goes beyond that perspective – to offer firms in Japan Positive Privacy Strategies. This is the approach that has been embraced by the best U.S. and Canadian

firms, and is aimed at enhancing customer trust and loyalty and winning a premier public reputation for the company in respect for its customers' privacy preferences.

The JPC also offers the expert perspectives of Professor Masao Horibe, Japan's leading legal expert on privacy and data protection; Russell Pipe, a long-time expert on data protection for Japanese companies and industry associations, and Vivian van Gelder, an expert on transborder data transfers and global privacy protection law and practices.

For information about the JPC,
please visit the Japan Privacy Resource at
www.PrivacyExchange.org.

An Invitation to Privacy Professionals

To Become a *P&AB* Privacy Fellow

And Participate in a Comprehensive, Integrated Program Delivering Support Throughout the Year For Corporate Privacy, Data Protection, Compliance, Government Relations, HR Information Officers and Those Involved in Privacy and Information Management

Who Should Be A Fellow?

As a CPO, or person with responsibilities in privacy, compliance, data and information security, or HR management, you have two responsibilities:

- To be on top of events and issues that affect your company
- To establish yourself as the "go to" person your company can rely on for privacy information.

Why YOU Should Join the Fellows Program?

To fill these important roles and lead effectively, you need:

- The very latest privacy news
- The best analysis of privacy legislation
- Opportunities to meet and exchange information and to network with others who share your mission
- To receive cutting-edge trend, survey and research reports.

Just Some of the Benefits*...

- Five free subscriptions to ***P&AB's*** Newsletter and NewsFlash
- One free ***P&AB*** report or survey
- One complementary admission to ***P&AB's*** National Conference and additional registrations at a discount
- Value - Beyond Dollars & Cents: Great savings to your organization and delivery of extremely valuable information and publications to you and your staff

** For full details and list of the PFP Benefits Package please refer to our website at www.pandab.org*

Join today and start saving!

Contact Olga Garey for special Privacy Fellows Program rates at

(201) 996-1154 or info@pandab.org

PRIVACY & AMERICAN BUSINESS
A Comprehensive Report and Information Service

LOOKING AHEAD

Alan Westin's Privacy Predictions for 2010