

# PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Volume 28 Number 15 August 11, 2008

*CAPITAL INSIGHTS: The Senate Appropriations Committee has approved a funding measure that threatens to withhold about \$400 million from the State Dept. in fiscal 2009 if it fails to implement all of the State Inspector General's recommendations for improving security for its passport information database. The vote was a response to the March news that three contractors and a State employee snooped into the passport files of three presidential candidates in violation of the 1974 Privacy Act. The violations and an ensuing investigation led State's inspector general to make 22 recommendations for how the agency's Bureau of Consular Affairs should improve security. Leading privacy advocates, including the ACLU, Electronic Privacy Information Center and Peter Swire, a law professor at The Ohio State University who served as a top privacy officer in the Clinton Administration, said the episode supported their view that the Privacy Act needed an overhaul to ensure that citizens' data were adequately protected. . . . A proposal (HR 5170) to require a privacy officer in each of the Homeland Security Department's components was approved by the House Committee on Homeland Security in June and sent to the full House. DHS has nine components, and four have full-time privacy officers, according to the bill co-sponsored by Reps. Christopher Carney (D-Pa.) and Bennie Thompson (D-Miss.). The divisions of DHS that have full-time privacy officers generate more Privacy Impact Assessments. Specifically, of the 11 components that have generated any PIAs, the three that have designated privacy officers account for 57 percent of the total. "The presence of a full-time Component Privacy Officer would ensure that privacy considerations are integrated into the decision-making process at all of the DHS Components," Thompson and Carney wrote.*

## MAJOR STORIES IN THIS ISSUE

**Two Firms Emerge As Leading  
Health 'Credit Bureaus' . . . . 2**

**Brill's Fast-Passenger Outfit  
Loses Customers' Data . . . . 6**

**Feds Charge Ring Over Hack  
Of TJX, Other Retailers . . . . 4**

**FOIA Ct Roundup: Time Limit;  
'Exigent Circumstances' . . . 7**

**In Brief: Texas AG Abbott Raps Radio Shack;  
California's Anderson Calls for Google-Yahoo Probe . . . 9**

## **PRESCRIPTION-DATA REPORTS ENABLE INSURERS TO JUDGE APPLICANTS**

Two competing companies in the Midwest are quietly accessing databases containing prescription drug records on millions of Americans, enabling them to sell health “credit reports” to health and life insurance companies evaluating applicants.

Ingenix, a Minnesota-based health information services company that had \$1.3 billion in sales last year – and Wisconsin-based rival Milliman IntelliScript – told the *Washington Post* that the drug profiles are an accurate, less expensive alternative to seeking physician records, which can take months and hundreds of dollars to obtain. They claimed that consumers authorize the data release in generalized consent forms and that the services can save insurance companies millions of dollars and benefit consumers anxious for a decision.

In February, the Federal Trade Commission issued an order saying that MedPoint and IntelliScript are consumer reporting agencies (CRAs) under the Fair Credit Reporting Act, so the companies must notify insurers that consumers denied insurance on the basis of their consumer reports have the right to request a copy of the report and that errors be corrected. The FTC’s order followed a settlement of allegations that the companies violated the credit-reporting law by failing to provide such notice to insurers.

However, the FTC rejected a recommendation by Pam Dixon, Executive Director, of the World Privacy Forum, that the companies should have been hit with civil fines, and required to directly notify consumers about the sale of their reports. Bob Gellman, an independent privacy consultant in Washington, told the *Post* that the FTC’s decision not to fine the companies sends “the message that it is okay to ignore the law.” That, he said, “is absolutely outrageous.”

Ingenix and Milliman create profiles by exploiting the databases of prescription drug histories kept by pharmacy benefit managers. PBMs help insurers process drug claims. Ingenix has servers in the PBM data centers and updates the drug files as frequently as once a day, said John Stenson, senior vice president of consulting for Ingenix, which is a division of UnitedHealth Group. The corporation also owns UnitedHealthcare, the nation’s second-largest insurer.

When an insurer makes an online query about an applicant, Ingenix or Milliman’s servers scour available data and within minutes or less return reports to a central server at the company. The server aggregates the information going back as far as five years, including the drugs and dosages prescribed, dates filled and refilled, the therapeutic class and the name and address of the prescribing doctor.

Then Ingenix’s MedPoint analysis tool provides insurers a “pharmacy risk score,” or a number that represents an “expected risk” for a group of people, such as 30- to 35-year-old women who have taken prescription drugs, Stenson said. Higher scores imply higher medical costs. Milliman’s IntelliScript codes drugs red, yellow or green, according to the insurer’s instructions, with red signaling the greatest risk, Mark Franzen, managing director of Milliman IntelliScript,

told the *Post*. Red codes could include the so-called AIDS cocktail drugs and cancer medications.

The companies receive data only on individuals who are in clients in PBMs' databases, generally excluding people who pay for drugs in cash. The profiles cost insurers about \$15 a search. IntelliScript gets about 1 million queries per year, largely from individual health insurers.

Some health experts said insurance companies can make faulty assumptions by looking at prescription drug records, because many drugs have multiple uses. "I had a patient on Amitriptyline for migraines and they were denied life insurance because it's also an anti-depressant," Kate Atkinson, an Amherst, Mass. Physician, told the *Post*. "I had to explain it wasn't being used for depression." Another patient was on Prozac – not for depression, but for menopausal hot flashes. "I wrote an appeal letter, and they still wouldn't give it to her," Atkinson said.

The system can save money for insurers, said Richard Dick, an entrepreneur who built the database system that Ingenix acquired in 2002. For instance, if MedPoint produces a report that an individual has been on the highest dose of the cholesterol-reducing drug Zocor for 18 months, the insurer "would be able to know that you have a very high, near-intractable cholesterol problem," Dick said, and could avoid a costly blood test.

Tia Goss Sawhney, a Chicago area health insurance actuary who has used both companies' tools, told the *Post* it was valuable to have access to an "objective" source of third-party information. "Though most people tell the truth most of the time, there are people out there who don't, who leave out something that's incredibly relevant, who may even be able to defraud a company," she said. A company would want to know if a consumer already was taking medications that cost \$400 every six months, industry experts said.

Franzen, whose firm expects revenue of \$575 million this year, said his clients tell him that about 10 percent of applicants do not disclose pertinent medical conditions in their applications that are later revealed by prescription drug history.

Neither the Ingenix nor Milliman IntelliScript Web sites indicated how consumers could request copies of their profiles. Franzen told *Privacy Times* in an email exchange that Milliman did not maintain a mega-database like traditional credit bureaus. Instead, it retrieves and assembles a consumer's data when ordered by insurers. Milliman would only have copies to give to consumers if a report had been purchased, he said. To obtain their reports, consumers need to provide their names, addresses, last four digits of their SSN to Milliman either by calling the toll free number 877-211-4816, or writing to Mark Franzen, Managing Director, Milliman IntelliScript, 15800 Bluemound Road, Suite 400, Brookfield, WI 53005

Ingenix had not responded to *Privacy Times*' queries by deadline.

**FEDS CHARGE PERPS WITH PENETRATING  
TJ MAXX, DSW SHOES, B.J.'s, SPORTS AUTHORITY**

The federal indictment of 11 individuals allegedly involved in the heist or sale of 40-plus million credit card and debit numbers highlighted the global scale of identity theft. Three of the defendants are U.S. citizens, one is from Estonia, three are from Ukraine, two are from the People's Republic of China and one is from Belarus. One individual is only known by an alias online, and his place of origin is unknown.

The indictments confirm that ring members were responsible for the highly publicized hack of TJX, owner of retailers TJ Maxx and Marshalls, the largest known attack of its kind that prompted a myriad of probes by State Attorneys General, as well as private lawsuits by consumers and banks.

The episode also drove home a less-noticed lesson: the potential link between security breaches at major retailers and the subsequent misuse of customer information. Targeted retailers included BJ's Wholesale Club, OfficeMax, and DSW Shoe Warehouse, all of which made the headlines in recent years as victims of security breaches. As is so often the case, in each instance, the retailer initially said there was no evidence that the compromised data had been misused.

Other targets included Boston Market, Barnes & Noble, Sports Authority, and Forever 21.

On Aug. 5, 2008, a federal grand jury in Boston indicted Albert "Segvec" Gonzalez, of Miami, on charges of computer, wire and access device fraud, aggravated identity theft and conspiracy for his role in the scheme. Christopher Scott and Damon Patrick Toey, both of Miami, were hit with related charges.

The Boston indictment alleges that Gonzalez and his co-conspirators obtained the credit and debit card numbers by "wardriving" and hacking into the wireless computer networks of major retailers. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks.

Once information was collected, the conspirators concealed it in encrypted computer servers that they controlled in Eastern Europe and the U.S. They allegedly sold some of the credit and debit card numbers, via the Internet, to other criminals in the U.S. and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The perpetrators then allegedly used these cards to withdraw tens of thousands of dollars at a time from ATMs. Gonzalez and others were allegedly able to conceal and launder their fraud proceeds by using anonymous Internet-based currencies both within the U.S. and abroad, and by channeling funds through bank accounts in Eastern Europe.

Gonzalez had quite a history. He was actually working as a confidential informant for the Secret Service, which previously had arrested him in 2003 for access-device fraud. The Secret

Service's investigation of TJ Maxx and other retailers convinced agents that Gonzalez was criminally involved once again. Gonzalez now faces a maximum penalty of life in prison if he is convicted of all of the most recent charges.

Indictments were unsealed simultaneously in San Diego against scheme participants Maksym "Maksik" Yastremskiy, of Kharkov, Ukraine, and Aleksandr "Jonny Hell" Suvorov, of Sillamae, Estonia. The indictments charged the defendants with illegal trafficking in credit card data stolen by Gonzalez and others, and with aggravated identity theft. Similar indictments were handed down against Hung-Ming Chiu and Zhi Zhi Wang, both of the People's Republic of China, and a person known only by the online nickname "Delpiero," also unsealed in San Diego. Also in San Diego, Sergey Pavolvich, of Belarus, and Dzmitry Burak and Sergey Storchak, both of Ukraine, were charged in a criminal complaint with conspiracy to traffic in unauthorized access devices. All are believed to be foreign nationals residing outside of the United States.

Yastremskiy, Suvorov, Chiu, Wang, Delpiero, Pavolvich, Burak and Storchak allegedly operated an international stolen credit and debit card distribution ring with operations from Ukraine, Belarus, Estonia, the People's Republic of China, the Philippines and Thailand. The indictment of Yastremskiy alleges that he received proceeds exceeding \$11 million from this criminal activity. These indictments were the product of a three-year undercover investigation conducted out of the San Diego Field Office of the U.S. Secret Service.

In May 2008, Gonzalez, Suvorov and Yastremskiy also were charged in a related indictment in the Eastern District of New York. The New York charges alleged that the trio was engaged in a sophisticated scheme to hack into computer networks run by the Dave & Buster's restaurant chain, and stole credit and debit card numbers from at least 11 locations. Specifically, the indictment alleged that the defendants gained unauthorized access to the cash register terminals and installed at each restaurant a "packet sniffer," a computer code designed to capture communications on a computer network. The packet sniffer was configured to capture credit and debit card numbers as this information was processed by the restaurants. At one restaurant location, the packet sniffer captured data for approximately 5,000 credit and debit cards, eventually causing losses of at least \$600,000 to the financial institutions that issued the credit and debit cards.

Gonzalez is currently in pre-trial confinement on the New York charges. Based upon the San Diego charges, Turkish officials apprehended Yastremskiy in July 2007 in Turkey when he traveled there on vacation. He has been in confinement since then in Turkey, pending the resolution of related Turkish charges, and the United States has made a formal request for his extradition. At the request of the Department of Justice, Suvorov was apprehended by the German Federal Police in Frankfurt in March 2008 on the San Diego charges when he traveled there on vacation. He is currently in confinement pending the resolution of extradition proceedings.

"So far as we know, this is the single largest and most complex identity theft case ever charged in this country," said Attorney General Michael Mukasey. "It highlights the efforts of the Justice Department to fight this pernicious crime and shows that, with the cooperation of our law

enforcement partners around the world, we can identify, charge and apprehend even the most sophisticated international computer hackers.”

### **BRILL’S EXPEDITED PASSENGER SERVICE LOSES LAPTOP WITH CUSTOMER DATA**

The Transportation Security Administration suspended a highly-touted private service from enrolling airline travelers in its Registered Travel program after a laptop computer containing the records of 33,000 people went missing.

Verified Identity Pass, a New York-based company, lost possession of the laptop July 26 at San Francisco International Airport. The laptop contained unencrypted pre-enrollment records of individuals’ names, addresses and driver’s license or passport numbers. Most of the individuals were online applicants.

The Registered Travel program allows customers to pass quickly through security checkpoints at 17 U.S. airports. Verified Identity Pass is headed by Steven Brill, the brash CEO who founded the company after the 9/11 attacks.

“We don’t believe the security or privacy of these would-be members will be compromised in any way,” Brill told Bloomberg News. Verified Identity Pass has more than 200,000 customers. It already started notifying the affected people about the breach. The laptop was stolen from a locked office in the airport, the company said.

### **FOIA CT. ROUNDUP: TIME LIMITS & ‘EXCEPTIONAL CIRCUMSTANCES’**

The following is a summary of recent court decisions under the Freedom of Information Act.

#### **Government Accountability Project (GAP) v. HHS & FDA**,: (07-1702)

**Court:** U.S. District Court for the District of Columbia  
**Judge:** Colleen Kollar-Kotelly  
**Documents:** Clinical study data regarding the drug Ciprofloxacin (Cipro)  
**Issue:** FOIA time limits, court order against further delayed responses  
**Date:** August 4, 2008

The court ruled that the Food and Drug Administration (FDA), a component of the U.S. Dept. of Health and Human Services and failed to demonstrate “exigent circumstances” and “due diligence” sufficient to justify an extension of FOIA time limits, known as an **Open America** stay.

The FDA argued that several factors warranted an 18-month extension, including the fact that the request for records on the drug Ciprofloxacin (Cipro) was assigned to the “complex track” of FDA’s FOIA Office, the Division of Information Policy Disclosure (DIDP).

But the Government Accountability Project (GAP) said the FDA could not claim an unexpected surge in volume because FOIA requests actually declined from 5,310 FOIA requests in 2003, to 5,156 requests in 2004; 4,050 in 2005; 3,335 in 2006 and 2,888 requests in 2007.

FDA countered that the numbers were “somewhat misleading because it does not reflect the size and complexity of the requests received, or DIDP’s backlog.” Processing time is prolonged because of the need to redact trade secrets and other confidential commercial data, as well as personal information. It also claimed its proactive approach under E-FOIA in making more documents electronically available explained the declining trend in incoming FOIA requests without a corresponding decline in workload.

“The Court is sensitive to the fact that DIDP processes large and complex FOIA requests, and these considerations are relevant in determining whether Defendants have demonstrated exceptional circumstances,” responded Judge Kollar-Kotelly.

“Defendants’ arguments, however, do not suggest that the FOIA requests have become increasingly or unexpectedly more complex as of late. Nor do Defendants suggest that requesters have only recently or unexpectedly begun including multiple requests in a single FOIA request. As such, the incoming FOIA requests facing DIDP do not appear to be a “deluge” of new requests, but rather appear to be, as Defendants themselves describe, a “stream of new FOIA requests,” and one that is actually decreasing over time.”

“As the D.C. Circuit explained in Open America, ‘exceptional circumstances’ exist when an agency faces an unexpected volume of requests for information and has insufficient resources to deal with those requests in the time frames set forth in the FOIA. Exceptional circumstances, however, do not exist where ‘a delay. . . results from a predictable agency workload of requests under this section, unless the agency demonstrates reasonable progress in reducing its backlog of pending requests,’” she wrote.

FDA argued that exceptional circumstances existed because it faced “multiple FOIA lawsuits, third-party subpoenas and discovery requests in litigation matters, a significant and unanticipated increase in the resources that DIDP must devote to responding to document requests made by Congress, and additional responsibilities as a result of EFOIA, Executive Order 13,392 and the 2007 FDA Amendments.”

But Judge Kollar-Kotelly disagreed, stating that none of these factors constituted an unpredictable agency workload, or that DIDP’s resources were insufficient to handle the job.

“Significantly, because [the FDA] does not provide the Court with any sense of whether DIDP faced or handled similar litigation requests in previous years, the Court cannot determine whether the 2007 litigation requests were unusual. Moreover, even if DIDP faced heightened litigation requests in 2007, because those requests were coupled with a decrease in FOIA requests over previous years, the Court cannot evaluate how DIDP’s current overall workload in 2008 compares with its workload in the past,” she wrote.

While rejecting its bid for a stay, Judge Kollar-Kotelly recognized that the FDA was faced with a substantial backlog and that Plaintiff's FOIA request is currently pending in the processing queue. Accordingly, she required the FDA to file a status report by September 5<sup>th</sup>, "advising the Court as to the volume of the requested records, where Plaintiff's FOIA request currently stands in the processing queue, i.e., the date by which Defendants expect to begin processing Plaintiff's FOIA request, and how long they expect it will take to process Plaintiff's request, so that the Court can set an appropriate processing schedule."

**South Yuba River Citizens League, et al. v. National Marine Fisheries Service:** (No. S-06-2845)

**Court:** U.S. District Court for the Eastern District of California

**Judge:** Lawrence K. Karlton

**Documents:** NMFS "biological opinion," Army Corps-Engineers compliance, Daguerre Pt. Dam

**Issue:** FOIA time limits, **Open America** stay

**Date:** June 20, 2008

The court declared illegal the National Marine Fisheries Service's (NMFS) practice of responding tardily to FOIA requests from two non-profit groups, enjoined it from disobeying FOIA time limits and ordered it to produce within 20 days a *Vaughn* index addressing the deliberative process privilege asserted for documents requested by plaintiffs' in October 2007.

Two California groups, South Yuba River Citizens League (SYRCL) and Friends of the River, sought records relating to the Yuba River, including NMFS's "biological opinions," Army Corps of Engineers compliance with those opinions, and the Corps' water diversion operations near Daguerre Point Dam.

NMFS never sought an extension, and though it disclosed some information within a month of a request, never fully responded until more than six months later. The two groups sought a declaratory judgment that NMFS's delays in responding to their FOIA requests were unlawful.

"Declaratory judgment is proper when there are purely legal questions at issue and if the judgment will clarify the legal issues and provide clarity to the parties and the public. When an agency has ignored statutory mandates, including deadlines imposed by statute, a declaratory judgment may be merited. Here, NMFS has repeatedly shirked its statutory responsibility to respond fully to plaintiffs' FOIA requests within the timeframe set by Congress, or at the very least, explain why a timely response was not possible. The consistency of these violations and the possibility that they might recur with plaintiffs' fourth, pending FOIA request show that a declaratory judgment is appropriate here," wrote Judge Lawrence K. Karlton.

Turning to Exemption 5, he said a *Vaughn* index was necessary because NMFS failed to show that draft memos were not shared with the public. If they were shared, they would no longer be pre-decisional.

“Second, defendants have not shown that each of the documents is deliberative in nature. Defendants’ Vaughn declaration describes each withheld item only cursorily and with only occasional references to the opinions and recommendations contained therein. They also fail to offer adequate explanation as to why certain contents of each of the documents – such as factual portions and bibliographies – cannot be segregated and released. The *Vaughn* declaration states that a reader could deduce the writer’s opinions, thoughts, and recommendations by reading even these portions. This overly cautious approach, however, has been roundly rejected by the courts,” he wrote.

However, Judge Karlton upheld the agency’s search. “While there appears to be questions of delay, and lack of training, I cannot conclude that plaintiffs have presented evidence of Defendants’ bad faith,” he wrote.

**IN BRIEF . . .**

**Texas AG Abbott Raps Radio Shack**

Texas Attorney General Greg Abbott continued his campaign against companies’ lax security, reaching settlement agreements in mid-July with Select Medical Corp. and RadioShack on charges the companies failed to protect their customers from identity theft. Under the two agreements, the State will receive nearly \$1.5 million that will ultimately fund future identity theft investigations and prosecutions. Both companies will strengthen their existing information security policies by implementing new employee training programs that highlight identity theft prevention and educate staff about proper document destruction protocols. Additionally, RadioShack agreed to conduct unannounced compliance audits at all of its Texas stores at least twice a year. Under Texas law, vendors must take specific precautions before discarding documents that include customers’ bank accounts, driver’s license and Social Security numbers.

Abbott’s office opened its investigation into Select Medical after the Levelland Police Department found more than 4,000 documents containing customers’ sensitive information in garbage containers behind a company site. The records discovered by authorities contained patients’ bank account numbers, sensitive medical evaluations, drug and alcohol testing verification results, plan of care forms, insurance verification sheets, and social and vocational therapy questionnaires. The state’s enforcement action against RadioShack began when State investigators learned that the retailer’s Portland location exposed thousands of customers’ Social Security numbers, credit and debit card information, names, addresses and telephone numbers by dumping records into a publicly accessible trash can. Documents recovered from the trash included a customer’s 1998 credit application and a receipt for a shredder one customer purchased to prevent identity theft.

**Anderson: Google-Yahoo Probe Needed**

Joel Anderson, a Republican State assemblyman from San Diego, has urged California Attorney General Jerry Brown to investigate privacy implications of Yahoo’s search-advertising

deal with Google. “The impact of such potential market concentration – in both Internet search and search advertising – left in the hands of one company, at the very least, warrants rigorous scrutiny. We must ensure that the proper consumer safeguards and transparency are put in place to protect privacy,” he said in the letter, sent July 18 and released publicly Tuesday. “The ability to ‘data mine’ online behavior in order to find specific consumers interested in specific products is a big part of Google’s revenue stream and business plan. If Google is allowed to control over 90 percent of Internet searches, those data-mining capabilities will be unmatched and will soon make it impossible for any competitor to crack Google’s stranglehold on Web advertising.” Yahoo, Google, and the California attorney general’s office didn’t immediately comment on the letter. Attorneys general from Florida, Arkansas, and Connecticut are reviewing the Yahoo-Google ad deal. The Justice Department also is scrutinizing the partnership.

Yahoo disagreed, telling *C/Net*, “Both companies have taken important steps in this agreement to ensure that user privacy is protected. Any suggestion that Google and Yahoo are merging vast databases of personal information is simply false. While we may share some search terms to obtain sponsored search results from Google, we will not share personal information about our users without consent,” Yahoo said, adding that it will remove the last quarter of a searcher’s Internet address before handing the search term to Google. “The Internet-advertising model does not work without the trust of our users – most of what we do is offered to consumers for free, and users can leave at any time. We can only succeed if our users trust us and our privacy policies.” Google agreed with Yahoo, stating it “takes privacy very seriously and has structured the agreement to provide ads through Google’s AdSense program in a way that ensures that personally identifiable information of individual Internet users will not be shared, combined, or merged by the companies.”

---

**YES** I Want To Subscribe & Save 10% Off The \$390 Annual Rate

\_\_\_\_\_ \$350 Per Year (23 Issues)  
 \_\_\_\_\_ \$670 2-Year (46 issues)

Name \_\_\_\_\_  
 Org. \_\_\_\_\_  
 Address \_\_\_\_\_  
 City/ST/ZIP \_\_\_\_\_

\_\_\_\_\_ Credit Card No. (Visa, MC or Amex)

Phone No. \_\_\_\_\_

\_\_\_\_\_ Expiration Date

(Or you can pay by Check or Purchase Order)

**Privacy Times**  
 P.O. Box 302  
 Cabin John, MD 20818  
 (301) 229-7002 [Ph] (301) 229-8011 [Fax]

evan@privacytimes.com — [www.privacytimes.com](http://www.privacytimes.com)

---