PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Volume 25 Number 3 February 3, 2005

CAPITAL INSIGHTS: The new Bush Administration budget will propose spending $125 million to test computerization of health records, more than twice what was being spent in the budget year that ends Sept. 30. "Most industries in America have used information technology to make their businesses more cost effective, more efficient and more productive -- and the truth of the matter is health care hasn't," Bush told the Cleveland Clinic Jan. 27. The Cleveland Clinic has been helping the government develop standards for medical computerization and President Bush heard from doctors who showed him some of the technology. The President also said ways must be found to safeguard medical records to protect against "people prying into them," the Associated Press reported. He was accompanied by New Health and Human Services Secretary Mike Leavitt, who said wider use of computers for medical information brings "lower costs and fewer mistakes." HHS also announced steps to require electronic prescribing options as part of the new Medicare prescription drug program that begins January 2006. . . . For the fifth year in a row, identity theft topped the Federal Trade Commission's list of most-reported frauds. The number of complaints about ID theft jumped 15 percent from the previous year, the agency said -- and represent about 40 percent of all complaints. Some 250,000 consumers complained to the agency about ID theft last year, up from 215,000 in 2003. . . The American Civil Liberties Union is leading broad-based opposition to the so-called "REAL ID bill" (HR 418), sponsored by Rep. Jim Sensenbrenner. The bill would force States to link drivers' licenses to immigration status in violation of existing policies, it charged. The bill would continue the troubling march toward making the drivers' license a de factor national ID card, it said. The House has set a Feb. 9 floor vote on the bill.

MAJOR STORIES IN THIS ISSUE

Kelly: Privacy Still Paramount At Homeland Security 1

RFID: Parents Battle School Over 'Tagging' Children 3

FCRA: Oregon Jury Awards $210,000 In ID Theft Case . . . 5

Privacy Act's SSN Curb Not For State, Local Agencies . . 6

FOIA Ct. Roundup: No CIA Secrecy For P.O.W. Abuse . 7

In Brief: Privacy Research; CPOs, RFID, FOI Fees . . . 8

FIRST ANNUAL DHS REPORT COVERS FOIA, PRIVACY ACT, PIAs & PRIVATE SECTOR DATA

In her first annual report, Homeland Security Chief Privacy Officer Nuala O'Connor Kelly vowed continued vigilance to ensure protection of individual rights, stating that her active oversight of controversial data practices would continue.

The 38-page report, released Jan. 31, reflected Kelly's wide-ranging statutory duties: Privacy and Freedom of Information Act compliance, Privacy Impact Assessments (PIAs), legislative and regulator review, oversight, training and complaints.

Kelly's report came on the eve of the confirmation hearing of Michael Chertoff to replace Tom Ridge as head the Dept. of Homeland Security (DHS). Chertoff, a federal appeals court judge, told the Senate Homeland Security and Governmental Affairs Committee, "I believe the secretary of Homeland Security will have to be mindful of the need to reconcile the imperatives of security with the preservation of liberty and privacy." Chertoff, 51, highlighted his work as special counsel in the New Jersey legislature in examining racial profiling, and as a private attorney representing poor defendants. He also promised to "respect those with whom you work" - a signal to the 180,000 employees he would lead as the nation's second Homeland Security secretary.

DHS was the first federal agency directed by statute to have a Chief Privacy Officer (CPO). Legislation passed by Congress at the end of 2004 mandates that all major federal agencies appoint CPOs. Kelly's inaugural report highlights the broad nature of the job.

Kelly previously issued a report on the controversial transfer of data on JetBlue airline passengers to the Transportation Security Administration (TSA). Kelly said she was now reviewing additional transfers by other airlines "to ascertain if they were accomplished in compliance with applicable privacy laws and regulations," and would issue another report.

Moreover, in response to "a substantial number of complaints," she is conducting "a full-scale review" of the MATRIX program (Multi-State Anti-Terrorist Information Exchange), a system of integrated law enforcement and commercial databases that has been funded through a cooperative agreement with the DHS Office of Domestic Preparedness. The results of that review will be made public in the near future through a forthcoming report," Kelly wrote.

On the Privacy Act front, DHS closed approximately 24,000 Privacy Act requests during FY 2003, the vast majority of which were processed by U.S. Citizenship and Immigration Services (CIS). DHS also had computer agreements, including CIS's SAVE Program, (Systematic Alien Verification for Entitlements Program) with California, Colorado, New York, New Jersey, the District of Columbia. and Massachusetts. There also is a matching program to verify foreigners' eligibility for Supplemental Security Income, Temporary Assistance for Needy Families, food stamps, Medicaid, unemployment and, educational assistance. The Coast Guard participates in two matching agreements with the Dept. of Defense, the Veterans Administration and the Social Security Administration to verify eligibility for supplemental security income payments and special veterans' benefits.

"During FY 2003, DHS personnel processed 160,902 FOIA requests (agencies that preexisted the creation of DHS merged on March 1, 2003). Seventy-two percent of these requests were answered with either a full release of records or a partial release, with the most common reasons for withholding information being privacy-related (Exemptions 6 and 7(C)) of the FOIA were used nearly 62,000 times)," Kelly wrote, citing the link for the annual FOIA report. http://www.dhs.gov/interweb/assetlibrary/FOIADHSFY2003AnnualReport.pdf.

Kelly devoted considerable attention to Privacy Impact Assessments (PIAs), calling them new tools in the tool belt of Chief Privacy Officers. She said PIAs typically must address at least

two issues: 1) the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system and 2) the protections and alternative processes for handling information to mitigate potential privacy risks.

"A PIA outlines salient points about new or existing information technology systems by answering questions about the information that will be collected, the opportunity individuals will have to redress information collected about themselves, who will be able to access the information, how the system and data will be maintained, what administrative controls will be in place, and how the decision to use a system was made," she continued.

"The Privacy Office has been instrumental in making the PIA process a focal point for privacy activities at DHS. By providing written and oral training in addition to specific guidance materials, the Privacy Office has enabled all DHS program offices to incorporate privacy into their fundamental program planning."

"From the initial drafting of a PIA to the final product, the Privacy Office has provided PIA leadership to DHS offices and components. A Privacy Office publication, *PIAs Made Simple*, is in use throughout the agency, and several PIAs for major DHS initiatives have set the standard for agency documents of this kind. In addition to PIA development for programs since April 2003, the Privacy Office has reviewed nearly 90 PIAs in connection with the OMB 300 process, which requires PIAs in connection with any funding request of more than $500,000 for new technologies or improvements on existing information systems and technologies."

"Additionally, the Privacy Office is reviewing PIAs, or advising on the need for their development, in connection with DHS rulemakings. Finally, as a policy matter, the Privacy Office may request that a DHS office or component undertake the preparation of a PIA to assist with a privacy review of a non-IT or rule-based proposal for a DHS program. The Chief Privacy Officer provides final agency review of PIAs before they are forwarded to OMB and then published in the Federal Register, or otherwise made publicly available," she wrote.

Citing the emphasis on protecting individual rights in the Declaration of Independence and the Constitution, Kelly said that DHS continued this tradition by serving as both a "counterterrorism" and "protective" agency.

"The senior leaders of this Department, with whom I am proud to serve, are committed to safeguarding the people and places of our country, as well as our liberties and our way of life. A significant part of safeguarding those liberties is protecting the dignity and the uniqueness of the individual. And protecting the dignity and uniqueness of the individual requires -- indeed demands -- that we protect the privacy of that individual," she concluded.

SCHOOL, SOME PARENTS AT LOGGERHEADS OVER MADATORY RFID TAGS FOR STUDENTS

A rural Northern California school has become the latest battleground over RFID technology, as a handful of parents are objecting to a surprise requirement that their children must wear a tagged card hanging from their neck as part of a new attendance program.

The one-school district in Sutter, Calif., has threatened disciplinary actions against two students who initially refused to wear the RFID "badges," but now are only required to wear "blank" badges which contain neither the RFID tag nor name, grade and photo worn by all other junior high-age students. Leading the fight are Mike and Dawn Cantrall, who advised the school orally and in a letter that they instructed their seventh-grade daughter and fifth-grade son not to wear the RFID badges.

The Cantralls raised several concerns about the RFID tags, including safety, security and religious beliefs.

"RFID is not new technology and is rapidly becoming the preferred method of inventory control in the retail sales and manufacturing industries," the Cantralls wrote in a Jan. 30 letter. "Yet, I can find no references of RFID being used to track elementary or junior high students in a California public school. Our children are NOT 'inventory.'"

In a Jan. 31 e-mail, Paul Nicholas Boylan, an attorney for the school board, said Brittan School Superintendent/Principal Earnie Graham is required to carry out the Board's directive to conduct the test.

"Until the Board has an opportunity to consider your complaints and alters their instructions -- or until a court order mandates a change -- the test will continue. All students are required to participate in the test, including your two children, (names' deleted)," he wrote.

"(Your two children's) participation in the test is minimal. In order to address your concerns regarding the test, (their) participation will not generate any information regarding them. All electronics have been removed from their tags. Moreover, unlike all other participants in the test, (their) tags have no name and no photograph. Their tag is, essentially, neutral and blank," he continued. "Nevertheless, they are required to wear their neutral tags during the test. Failure to do so will possibly result in disciplinary action against (them)."

In a separate e-mail to a different parent who raised concerns, Boylan wrote: "Frankly, no opposition was anticipated. The District is being given the opportunity to help pioneer an automatic attendance system that will not only save money and free up teacher time for additional instruction, but it will also enhance school safety. It is likely that this system will eventually be mandated for all public schools in California. We have a chance to create the standards for this new system instead of having standards imposed upon us. Moreover, this is only a test for a limited time. It may or may not prove effective. If it does, then the District will have the option of setting up a permanent system -- again at no expense to the District.

The School Board has set a Feb. 8 meeting to consider the Cantralls' complaints. The meeting could prove crucial in deciding the fate of the RFID program, as well as the fate of any child who refuses to participate. School Board President Don Hagland did not respond to *Privacy Times'* inquiries.

The program was launched after Bernie DiDario, president of a local RFID company, InCom Corp., approached the school. DiDario said that with RFID antennas at each classroom door and each student wearing an RFID tag, the system could record all students who were "present," send the information to an InCom server, which would relay the information to the teacher's Dell Personal Digital Asst. (PDA), and then to the principal's office in the form of an

attendance report. DiDario donated $2,500 and the PDAs. Sources said that two teachers at the local public high school were involved in the development. A photo of Brittan students with the badges hanging from their necks is at the company Web site, www.incomcorporation.com.

A seven-classroom test began in mid-January with little fanfare. In the Jan. 26 weekly newsletter to parents, a box entitled, "New Safety I.D. Badges," it read:

> On Tuesday, Jan. 18th, every student will be issued 'an I.D.' badge. It is important that the badge be worn at all times during normal school hours. This additional safety step will help keep your child safe while at school. It will not only help with knowing if we have non-students on campus, but in emergency situations, every student could be identified by any staff member or by law enforcement or fire personnel. The badges are very durable, but students who lose or destroy their badges will be accountable for the cost of replacing them. Thank you for your support in keeping all of our students safe.

The newsletter did not initially mention that RFID was involved, or that antennas also were installed in school bathrooms.

After the Cantralls objected, the school still required their children to wear cards lacking their identifiers and the RFID tag. Graham summoned the fifth grader to his office to give him a note permitting him to attend school with a blank ID card. He acknowledged telling the Cantralls' son of the benefits of wearing the RFID tag, but the youngster held firm and declined.

Opposition among parents seemed to be growing. Concerned parents set a Feb. 3 evening meeting to discuss the matter in advance of the School Board's Feb. 8 meeting.

Meanwhile, the InCom Corp. has is looking beyond the rural school district. The press release at its Web site proclaims that it has several patents pending for the product, known as "InClass." It described RFID as a "state of the art method for identifying, locating and tracking in all types of environments, such as hospitals, office buildings, amusement parks, and now schools."

According to co-inventor Doug Ahlers, "InClass" not only improves the accuracy of attendance reporting, but allows that "students can be quickly located and summoned with the (PDA) handhelds."

Michael Dobson, a company founder, "We have devised a number of innovations for the school environment … We believe this system will have many applications outside of the classroom," he said. InCom will demonstrate the product at the Feb. 19 annual convention of the American Association of School Administrators (AASA) in San Antonio, the press release said.

In his letter, Cantrall pointed out that "the newest game at school is 'tag' where kids try to grab the ID card and pull it off another kid's neck. It has also been reported by students that some of the lanyards are already broken and students are tying knots in the cords."

Graham, the School Superintendent, agreed that the devices were not popular among the kids, and also said there were glitches in the system.

"This whole thing might not work. That's why we are testing it. There's no hidden agenda. My concern is to reduce the time needed for taking attendance so teachers have more time to teach, and to improve safety for the kids," he said.

But James P. Harrison, a privacy attorney in Sacramento, commented, "This case in point of trading human dignity and basic privacy for questionable efficiency sets a dangerous example for our children and our communities."

FCRA: OREGON JURY AWARDS $210,000 TO ID THEFT VICTIM IN EQUIFAX CASE

A federal jury in Portland, Oregon has awarded $210,000 in actual damages to a victim of identity theft who sued Equifax under the Fair Credit Reporting Act (FCRA) for failing to remove some fraud-related accounts from his credit report. The jury declined to award punitive damages against Equifax. Although an appeal was possible, it was seen as unlikely by most observers.

The case arose in 2000 when Matthew Kirkpatrick learned he had become a victim of identity theft due to fraud committed by someone in Coeur d'Alene, Idaho. Kirkpatrick, a construction worker, assembled a dispute package that included police reports, copies of his driver's license and Social Security card, letters from creditors stating that he was not responsible for bad debts, and documents showing which accounts were fraudulent and needed to be removed.

Equifax initially responded with a letter stating that it had "shredded" Kirkpatrick's dispute package. Equifax later testified that it shredded it for security reasons after it was unable to locate his file. Kirkpatrick sent Equifax the same dispute package three more times. For the final package, he received the U.S. Postal Service's "return receipt" confirming that Equifax received it. But each time he called, Equifax said it could not locate his dispute package.

Kirkpatrick's phone disputes were unable to clear up his credit report. His efforts continued over several years. Meanwhile, the credit report errors prevented him from obtaining the credit he needed to complete an addition to his house. Kirkpatrick's wife was pregnant with their third child and he had begun work on a new bedroom. The addition remained uncompleted for two years. Kirkpatrick finally filed suit, testifying at trial that Equifax's dispute process was frustrating, humiliating and stressful.

At trial, Equifax admitted that it performed badly. Alicia Fluellen, the head of Equifax's dispute department, referred to Kirkpatrick's case as the "Murphy's Law" of disputes, testifying that everything that could go wrong, did. While Fluellen testified that she was "embarrassed" by the string of mistakes, she was steadfast in defending Equifax's overall system, stating that she had seen it work well through the years.

The trial testimony shed new light on some of Equifax's inner workings, including its system for outsourcing consumer disputes to Jamaica and Canada. *Privacy Times* Editor/Publisher Evan Hendricks gave expert testimony for Kirkpatrick relating to the history of credit report inaccuracy, the prevalence of identity theft and what he saw as shortcomings in Equifax's mainly automated system for handling consumer disputes.

Kirkpatrick was represented by Michael Baxter and Robert Sola, who in 2001 won a

$5 million punitive damages verdict against Trans Union in a mixed file case. The judge in the case reduced it to around $1 million and Trans Union paid. Equifax was represented by Kilpatrick & Stockton of Atlanta; Mara McRae was lead counsel.

COURT: PRIVACY ACT'S SSN CURB DOESN'T APPLY TO STATE OR LOCAL AGENCIES

A federal appeals panel has ruled that that a Privacy Act restriction on the using Social Security numbers does not apply to State and local governmental agencies, despite plain language in the statute to the contrary.

The opinion, by a three-member panel of the U.S. Court of Appeals for the Sixth Circuit, dismissed a lawsuit against the City of Detroit over the inclusion of SSNs on envelopes sent by its vendor to local taxpayers. Detroit Mayor Kwame Kilpatrick responded to the highly publicized faux pas with a letter to aggrieved taxpayers promising to "take the necessary steps to prevent such an unwelcome event in the future."

Daniel A. Schmitt sued under Privacy Act Sect. 7(b), which provides, "Any Federal, State or local government agency which requests an individual to disclose his SSN shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

"However, the language of § 7(b) suggesting that state and local agencies fall within its ambit is at odds with another crucial definition of the Privacy Act, as codified at 5 U.S.C. § 552a," the court noted.

Specifically, it said, the Privacy Act definition came from that of the Freedom of Information Act, namely an "executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency."

"In short, the Privacy Act, albeit by reference, unambiguously defines the term 'agency' as an agency of the federal government," wrote Judge Alan E. Norris, who was joined by Judges Deborah L. Cook and Sandra S. Beckwith

"We are therefore confronted by two provisions of the Privacy Act that contradict one another to some degree: the statutory definition, which unambiguously contemplates that the Privacy Act applies exclusively to federal agencies, and § 7(b), which by its terms includes State and local agencies within its ambit," he continued

"When faced with statutory sections that are inherently inconsistent, our first duty is to reconcile the competing provisions so that they can both remain in effect. In this case, however, such a reconciliation is impossible. The statutory definition of an agency found at § 552a(a)(1) contains no language to indicate that it does not apply to the Privacy Act as a whole. Were we to hold that § 7(b) applies to state and local agencies, we would effectively say that an unambiguous definition of a core term, which itself was promulgated by Congress, applies only part of the time. This we will not do." (***Daniel A. Schmitt v. The City of Detroit***.: CA-6 – No. 03-1884; Jan. 14.

FOIA CT. ROUNDUP: RED CROSS & GUANTANAMO; GRAND JURY

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

American Civil Liberties Union v. U.S. Dept. of Defense: (No. 04 Civ 4151)
Court: U.S. District Court for the Southern District of New York
Judge: Alvin K. Hellerstein
Exemptions: FOIA (b) (1), classified data; (3), sensitive data from Intl. org; & (5)
Documents: CIA documents on treatment of detainees at U.S. facilities
Issue: CIA 'Operational Files' exemption
Date: February 2, 2005

The court rejected the CIA's attempt to shield documents about alleged abuse of detainees under its special exemption for "operational files," finding that for starters, the CIA Director never personally invoked the exemption as required by law.

Judge Alvin Hellerstein found even if they were properly deemed to be "operational files," they would have been subject to the FOIA because they involved an investigation into wrongdoing by the CIA Inspector General. He also found the CIA already had performed a search of its operational files.

The CIA argued that it could not search for pertinent files until IG finished his investigation. "These administrative concerns, likely to arise whenever operations are investigated, reflect a reluctance on the part of the CIA to comply with [Operational Files Exemption – section 431(c)(3)]. The CIA's reluctance to comply with FOIA is not a lawful excuse," he wrote.

He ordered the CIA to either justify secrecy under the regular FOIA exemptions, or disclose the documents.

IN BRIEF . . .

Privacy Research In Canada

The Privacy Commissioner of Canada has awarded $371,590 to non-profit organizations and trade associations to support research into the impact emerging technologies have on privacy. Jennifer Stoddart, the commissioner, said in a statement that due to the quality of the submissions the commissioner's office added an additional $171,590 to the original $200,000 budget. "Canadians are becoming increasingly aware of privacy threats in an age of global and inter-organizational transmission of personal information," Stoddart said. "This is the first time the OPC has launched a program to enhance knowledge in addressing those concerns, by building strong links between the research community and privacy rights practitioners in Canada," she said.

The ten recipients, who received awards ranging from $50,000 to $14,603, include the Canadian Marketing Association to help businesses develop best-practices to handle customer data; the Ecole nationale d'adminstration publique to study the use of video surveillance cameras

in Canada; the British Columbia Freedom of Information and Privacy Association to study information technology weaknesses that lead to identity theft; the University of Victoria to study the privacy implications of location-based services; and Simon Fraser University to study regulatory measures to eliminate anonymous prepaid communications services.

RFID & GSA

Federal government agencies should further the development of the fledgling Radio Frequency Identification (RFID) industry by urging suppliers to deploy RFID technology on all current and future government contracts, according to a General Services Administration "Bulletin." The Dec. 4 directive, signed by G. Martin Wagner, GSA Associate Administrator, encourages agencies "to consider action that can be taken to advance the [RFID] industry by demonstrating the long-term intent of the agency to adopt RFID technological solutions." The directive lets agency heads make exemptions for the defense and aerospace industries and others critical suppliers that can not retool in time.

Katherine Albrecht, founder and director of Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), said "Buying needed equipment is one thing. Finding excuses to purchase and promote controversial technology at taxpayer expense is another … The RFID industry has planned to use 'top tier' government officials to advance their agenda since 2002," she said in a January 31 statement. Given recently announced initiatives by the Social Security Administration, NASA, the Postal Service and the Homeland Security Department, "apparently those efforts are now paying off," Albrecht said. She pointed to a cache of confidential documents that her group discovered in 2003. These included a strategy document prepared for a prominent RFID industry consortium by public relations firm Fleischman-Hillard. The document recommended identifying "key government, regulatory, and interest group leaders" to bring into the "inner circle" of support for the RFID industry. In one of the confidential documents, Fleischman-Hillard indicated that there had even been a "successful meeting with Office of Homeland Security Director Tom Ridge."

More, Less ID Theft

A study commissioned by the financial services industries found that 9.3 million people in the United States were victims of identity theft in 2004, below the 10.1 million victims predicted by the Federal Trade Commission. The study, commissioned by CheckFree Services Corp., Visa USA and Wells Fargo Bank and conducted by the research firm Javelin Inc., found that more people fell victim to identity theft from offline, rather than online commerce and transactions.

But others disagree with the study's findings. Avivah Litan, an analyst with the Gartner Group, told MSNBC that consumers often don't know how their personal information is stolen, especially regarding credit card fraud. "The study is biased towards people who know how it happened," she said.

Davis Vow Pushback On U.S. CPOs

Rep. Tom Davis, chairman of the House Government Reform Committee, plans to eliminate a provision in the 2005 omnibus spending bill calling for the creation of chief privacy officer positions.

"These privacy officers have got to be put into perspective," Davis told Federal Computer Week in a January 13 interview. "If you want to have them, fine. But let's not make it so confusing that the [chief information officers] basically lose control of information security and privacy becomes the overriding concern." Davis said he "doesn't have the concern that we need a [CPO], another bureaucrat," and that these positions were the initiative of Sen. Richard Shelby (R-Ala.). "The privacy officers, I guess, are a way to try to offer the public some kind of protection that the information they're giving the government is not going to be misused," Davis said. "But for the life of me, if that's what they wanted to do, that's not what they did in this legislation. And if that's what they want to do, we'll write it, and we'll have them do what they want to do. But let's just do that, and let's not do 10 other things that were unintended," he added.

$400,000 FOIA Search Fee

A public interest group seeking to determine the number of immigrants whose cases were declared secret after being arrested by the U.S. government following the September 11 terrorist attacks has been socked with an enormous research fee that may stymie the case.

The Justice Department has told the People for the American Way (PFAW) that it must pay a nearly $400,000 research fee before the government will compile the records the group seeks under the Freedom of Information Act. "Apparently, they've taken the 'free' out of 'freedom of information,'" said Ralph G. Neas, the foundation's president, in a statement. "If you want to learn about secret trials carried out by your government with your money, you are going to need deep pockets," he added, noting that prohibitive FOIA fees is the latest tactic by the Justice Department to hide information from the public. "It begs the question: what are they hiding?" PFAW first filed the FOIA request in November, 2003, which the Justice Department initially denied on privacy grounds but decided to meet before PFAW filed a lawsuit to compel disclosure. Neas said PFAW will appeal the fee. "We're going to fight this outrageous demand," he said.