PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Volume 29 Number 3 January 30, 2009

*CAPITAL INSIGHTS: As Privacy Times forecast last issue, current Commissioner **Jon Leibowitz** has emerged as the Obama Administration's leading candidate for Chairman of the Federal Trade Commission. Leibowitz was an influential Senate staffer before being named FTC commissioner in September 2004. Once the chairman is finally chosen, the FTC will move to fill other important posts, including the head of consumer protection . . . The other leading candidate for Chair was former Commissioner **Christine Varney**, a Hogan & Hartson partner who recently served as personnel counsel for the Obama transition team. But Varney was named to head the Justice Dept.'s Anti-trust Division.*

MAJOR STORIES IN THIS ISSUE

BACK TO THE FUTURE: OBAMA DIRECTS DoJ TO REVISE FOIA GUIDANCE

In his first days in office, President Obama signaled a new era of openness by ordering federal agencies to "adopt a presumption in favor of disclosure, in order to renew their commitment to the principles embodied in the FOIA." New guidance from the Justice Dept. will follow, he said.

The move, like most of Obama's earliest actions, represents a 180-degree pivot away from the Bush Administration's pro-secrecy policies. The Bush Justice Dept. guidance essentially encouraged agencies to err on the side of non-disclosure.

"The Freedom of Information Act should be administered with a clear presumption: In the face of doubt, openness prevails," Obama stated.

"The Government should not keep information confidential merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears. Nondisclosure should never be based on an effort to protect the personal interests of Government officials at the expense of those they are supposed to serve. In responding to requests under the FOIA, executive branch agencies (agencies) should act promptly and in a spirit of cooperation, recognizing that such agencies are servants of the public."

Obama directed the Attorney General to "issue new guidelines governing the FOIA to the heads of executive departments and agencies, reaffirming the commitment to accountability and transparency, and to publish such guidelines in the *Federal Register*."

"In doing so, the Attorney General should review FOIA reports produced by the agencies under Executive Order 13392 of December 14, 2005. I also direct the Director of the Office of Management and Budget to update guidance to the agencies to increase and improve information dissemination to the public, including through the use of new technologies, and to publish such guidance in the Federal Register."

"A democracy requires accountability, and accountability requires transparency. As Justice Louis Brandeis wrote, 'sunlight is said to be the best of disinfectants.' In our democracy, the Freedom of Information Act, which encourages accountability through transparency, is the most prominent expression of a profound national commitment to ensuring an open Government. At the heart of that commitment is the idea that accountability is in the interest of the Government and the citizenry alike."

MORE DETAILS SURFACE ABOUT SURVEILLANCE BY BUSH NSA

Russell Tice, the former National Security Agency employee who in 2005 blew the whistle on the agency's warrantless surveillance program, has resurfaced to provide more explosive allegations.

According to Tice, NSA spied on individual U.S. journalists, entire U.S. news agencies as well as "tens of thousands" of other Americans. His comments were first aired on Keith Olbermann's MSNBC news program. Tice wouldn't disclose the names of the specific reporters or media outlets that were targeted when he worked as an analyst for the NSA.

Moreover, Tice said the NSA had vacuumed in all domestic communications of Americans, including, faxes, phone calls and network traffic, and that the spy agency also combined information from phone wiretaps with data that was mined from credit card and other financial records. He said information of tens of thousands of U.S. citizens is now in digital databases warehoused at the NSA.

"This [information] could sit there for ten years and then potentially it marries up with something else and ten years from now they get put on a no-fly list and they, of course, won't have a clue why," Tice said.

In most cases, the person would have no discernible link to terrorist organizations that would justify the initial data mining or their inclusion in the database.

"This is garnered from algorithms that have been put together to try to just dream-up scenarios that might be information that is associated with how a terrorist could operate," Tice said. "And once that information gets to the NSA, and they start to put it through the filters there . . . and they start looking for word-recognition, if someone just talked about the daily news and mentioned something about the Middle East they could easily be brought to the forefront of having that little flag put by their name that says 'potential terrorist.'"

Tice's latest allegations add another piece to the Bush-NSA surveillance puzzle. The tense 2004 hospital showdown between then-White House Counsel Alberto Gonzales and Deputy Attorney General James Comey over the legality of a government surveillance program involved the mining of massive databases, according to a 2007 *New York Times* article. Tice was one of the sources for the *Times'* 2005 scoop on NSA surveillance.

New York Times reporter James Risen, who co-authored that paper's 2005 story on the warrantless wiretapping program with colleague Eric Lichtblau, told Olbermann he could have been among those monitored, noting that Bush Administration officials obtained copies of his phone records, which they showed to a federal grand jury. The grand jury is investigating leaked information that appeared in Risen's 2006 book *State of War* about a CIA program, codenamed Operation Merlin, to infiltrate and destabilize Iran's nuclear program. Risen doesn't know if his records were obtained by the FBI with a legitimate warrant or through the NSA program that Tice described.

Risen said the NSA program to monitor journalists was likely intended to help ferret out and intimidate possible sources and "to have a chilling effect on potential whistleblowers in the government to make them realize that there's a Big Brother out there that will get them if they step out of line."

More details about domestic surveillance are expected. *New Yorker* investigative reporter Seymour Hersh said prior to President Obama's inauguration that he had several sources waiting to talk. "You cannot believe how many people have told me to call them on January 20. [They say,] 'You wanna know about abuses and violations? Call me then,'" Hersh told a reporter.

ANOTHER PAYMENT PROCESSOR HIT BY MONSTROUS DATA BREACH

Major credit card issuers are reeling from what could turn out to be the biggest data breach ever. On Jan. 20th, Heartland Payment Systems, a New Jersey-based credit card processor, revealed that intruders cracked the system it uses to process 100 million card transactions per month from 175,000 merchants.

Robert Baldwin, Heartland's President and CFO, told *USA Today* that Visa and MasterCard were "instructing many card issuers" to offer fraud-monitoring protection, replace cards, or do a combination of both for customers whose card purchases were processed by Heartland. "We're heartsick over this," Baldwin said.

On Jan. 23rd, Bank of America and Heartland Bank said they were issuing new credit and debit cards to their customers in response to the security breach

Heartland Payments, reportedly the sixth largest credit-card processor, said on its Web site it did not yet know how many card numbers were obtained, and called many reports in the press "speculative." The data compromised included the information on a card's magnetic strip – card number, expiration date and some internal bank codes – that could be used to duplicate a card.

It did not include confidential merchant data, Social Security numbers, unencrypted personal identification numbers (PIN), addresses or telephone numbers, the company said.

Uncertainty over the duration of the hackers' penetration is driving speculation over the potential enormity of the breach.

Representatives of Visa Inc. and MasterCard Inc. alerted Heartland to a pattern of fraudulent transactions on accounts the processor handled sometime last fall, Baldwin told the *Wall Street Journal*. But initial internal investigations and audits failed to detect a security breach.

In mid-January, however, a forensic investigator discovered evidence of the breach. Heartland was targeted with malicious software that was "light-years more sophisticated" than malevolent programs commonly downloaded from the Internet, Baldwin said. Heartland said it had removed the malware and is working with the U.S. Secret Service to investigate the incident.

In November, *Privacy Times* reported that Citibank notified millions of cardholders that it was reissuing their credit cards because of an unspecified security issue, about which Citi declined to elaborate when we questioned them (see Vol. 28 No. 21, Nov. 17, 2008).

Citi Spokeswoman Janis Tarter still declined to confirm whether the Heartland breach was the cause of its sudden re-issuance of cards. But she said that Citi pays close attention to security

warnings from Visa and MasterCard, many of which do not identify the source of the breach or security problem. If indeed a Heartland-related warning prompted its preemptive actions, then it appears that Citi acted well ahead of others.

TJX Cos., operator of retailers TJ Maxx and Marshals, is the target of the biggest known breach, involving data on up to 45 million credit cardholders. After settling lawsuits by plaintiffs and card-issuing banks, and State Attorneys General, the breach reportedly thus far has cost TJX tens of millions of dollars – if not more.

The fact that Heartland's systems were certified as being fully in compliance with data handling rules, called the PCI standards, raises questions about the efficacy of such standards. Hannaford Brothers grocery chain was likewise fully PCI compliant when it had 300 stores hacked and 4.3 million record swiped.

Depending on the results of the ongoing investigation, Heartland is likely to face the threat of litigation from issuing banks, merchants and consumers. Chimicles & Tilellis of Haverford, Penn. was the first plaintiffs' firm to file a potential class action suit in U.S. District Court for the District of New Jersey.

"Consumers will know if their card account numbers have been used by reviewing their monthly statements, Heartland said in a statement. "Cardholders should report suspicious activity to their issuing banks (the bank that issued the card, not the card brand). If unauthorized use is confirmed, cardholders are reimbursed for the fraudulent purchases and are not held financially responsible."

In the days following the breach, Robert O. Carr, Heartland's founder and CEO said he had been talking to many industry leaders about working together to fight the cyber criminals who victimized Heartland and continue to jeopardize companies, consumers and data worldwide.

"Up to this point, there has been no information sharing, thus empowering cyber criminals to use the same or slightly modified techniques over and over again. I believe that had we known the details about previous intrusions, we might have found and prevented the problem we learned of last week," he said

"Heartland's goal is to turn this event into something positive for the public, the financial institutions which issue credit/debit cards and payments processors," he continued. "Just as the Tylenol crisis engendered a whole new packaging standard, our aspiration is to use this recent breach incident to help the payments industry find ways to protect its data — and therefore businesses and consumers — much more effectively."

According to a Heartland statement, Carr for the past year has been a strong advocate for industry adoption of end-to-end encryption — which protects data at rest as well as data in motion

— as an improved and safer standard of payments security. While admitting this technology does not wholly exist on any payments platform today, he said Heartland has been "working to develop this solution and is more committed than ever to deploying it as quickly as possible."

BOCKSTEIN HEADS NY EFFORT TO HELP IDENTITY THEFT VICTIMS

The New York State Consumer Protection Board (CPB) has launched a new Identity Theft Prevention and Mitigation Program designed to provide resources to help residents prevent identity theft and real-time assistance to victims in overcoming the consequences of this crime.

In addition to a central repository of identity theft-related resources and tools, the program offers consumer advisers that are trained to intervene and troubleshoot in various contexts, including creditors, financial institutions, credit-reporting agencies, utilities and employers.

''No longer will New York consumers who are already on overload dealing with the fallout of identity theft need to hunt for assistance and information,'' said Mindy A. Bockstein, State Consumer Protection Board chairperson and executive director. "Thanks to the actions of Governor Paterson and the New York State Legislature, victims can now turn to the CPB's Identity Theft Prevention and Mitigation Program to receive direct assistance and key information that can save them time, money and additional aggravation."

Under a new State law, victims of identity theft for the first time may be entitled to restitution equal to the value of the time they spend fixing the damage of identity theft under a new law. The Federal Trade Commission has estimated that it can take tens or even hundreds of hours to resolve problems associated with identity theft.

The Consumer Protection Board developed two journals to help victims detail the expenses related to the hours spent on repairing the damage done to their financial records and credit standing: the Identity Theft Victim Journal and the Identity Theft Victim Restitution Journal.

Another potentially effective tool featured in Gov. Paterson's identity theft initiative is an enhanced New York's Security Freeze law, making it easier for consumers to place a "freeze" or lock on disclosure of their credit reports. Credit reporting agencies must comply with such requests within three business days. The CPB is statutorily responsible for monitoring the time and technology it takes to place and remove a security freeze in New York State.

The new law further extends important confidentiality protections to Social Security numbers used by public entities and employers. Other resources include the Board's first "Business Privacy Guide: How to Handle Personal Identifiable Information and Limit the Prospects of Identity Theft." The guide explains some of the core privacy and security principles

as well as laws applicable to businesses and provides best practices to achieve compliance. New York is only one of three States to provide guidance to businesses on the use and secure retention of personal identifiable information. (www.nysconsumer.gov)

FISA COURT UPHELD SOME BUSH-NSA SURVEILLANCE

The secret "FISA" appeals court ruled last August that federal agencies can be authorized to conduct warrantless e-mail and telephone surveillance without violating the U.S. Constitution. But the court is so secret that its 29-page redacted opinion wasn't released until Jan. 15th

The court ruled that Presidents do not need to obtain warrants to conduct "foreign intelligence for national-security purposes" – which is effectively at least a partial endorsement of President Bush's views on expansive executive powers.

The central question in this case was how the Fourth Amendment's prohibition on "unreasonable searches and seizures" applies to intelligence agencies wishing to compel AT&T and other providers to open their networks to federal requests to listen in on international communications.

The case arose because an unnamed telecommunications company believed that surveillance was unconstitutional, particularly in light of the expiration of the "Protect America Act" in February 2008. The August 2007 law expanded the Foreign Intelligence Information Act and allowed warrantless eavesdropping on people "reasonably believed" to be outside the United States. It permitted the Attorney General and the director of national intelligence to issue directives – valid for one year – to force communications providers to open their networks for that purpose. The law expired on February 16, 2008, and was eventually repealed. It was revised in July 2008. But the directives issued during that time were still in effect, which led to the court challenge.

The U.S. Foreign Intelligence Surveillance Court of Review concluded that as long as the executive branch has "several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts."

Meanwhile, on January 15th, Attorney General-designate Eric Holder answered questions about warrantless wiretapping during his Senate confirmation hearing. Holder indicated that he would seek curbs on such National Security Agency programs.

FOIA CT. ROUNDUP: GITMO, ARMYCORPS, EPA, USDA, DHS, CIA, DoT, OMB

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

Associated Press v. Dept. of Defense, Dept. of Army: (No 07-5318)
Court: U.S. Court of Appeals for the Second Circuit (New York)
Judges: Peter W. Hall, Ralph K. Winter & Mark R. Kravitz
Exemptions: FOIA (b)(6) & 7(C), privacy
Documents: Identities of abused Guantanamo detainees
Date: January 5, 2009

The appeals panel ruled the Defense Dept. could withhold the identities of abused Guantanamo detainees, finding that detainees and their family members had a measurable privacy interest in their identifying data and that the Associated Press (AP) failed to show how the public interest would be served by disclosure. The decision reversed a lower court, which concluded that disclosure was in the public interest.

"The first question to ask in determining whether Exemption 7(C) applies is whether there is any privacy interest in the information sought," the panel wrote.

"The Supreme Court has explained that such privacy interests include 'the individual interest in avoiding disclosure of personal matters' as well as 'the interest in independence in making certain kinds of important decisions,'" it continued, citing ***Reporters Comm***., (489 U.S. at 762). "It further explained that 'both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person,' and thus that there is a recognized 'privacy interest in keeping personal facts away from the public eye,' It is well established that identifying information such as names, addresses, and other personal information falls within the ambit of privacy concerns under FOIA."

"As for the public interest against which the privacy interest is to be weighed, the Supreme Court has made clear that there is only one relevant interest, namely, 'to open agency action to the light of public scrutiny.'"

"The public interest 'cannot turn on the purposes for which the request for information is made,' and 'the identity of the requesting party has no bearing on the merits of his or her FOIA request.' Whether the public interest in disclosure warrants the invasion of personal privacy is determined by the degree to which disclosure would further the core purpose of FOIA, which focuses on 'the citizens' right to be informed about what their government is up to.'"

The panel concluded that detainees "certainly have an interest in both keeping the personal facts of their abuse from the public eye and in avoiding disclosure of their identities in order to prevent embarrassment."

"As victims of abuse, they are entitled to some protection of personal information that would be revealed if their names were associated with the incidents of abuse. The disclosure of their names could certainly subject them to embarrassment and humiliation."

It disagreed with the district court's conclusion that detainees did not have any substantial privacy interest because they, like prisoners, have little reasonable expectation of privacy.

"Although the detainees here are indeed like prisoners, their Fourth Amendment reasonable expectation of privacy is not the measure by which we assess their personal privacy interest protected by FOIA. Rather, the privacy interest for purposes of Exemption 7(C) is broad and encompasses 'the individual's control of information concerning his or her person.'"

"Moreover, the district court's reasoning that the detainees allegedly abused would want their plights publicized is also inapposite to the privacy interest at stake here. That a detainee might want to voluntarily disclose information publicly does not authorize the government to disclose that information, and the district court cites no law to support that proposition, nor do we find any," the panel wrote.

"This Court has similarly said that 'disclosure of information affecting privacy interests is permissible only if the information reveals something *directly* about the character of a government agency or official.'"

The AP argued disclosure was in the public interest because the information is necessary to shed light on the detainees' nationalities and religions and therefore provide context for DoD's response to the abuse allegations. It would also allow the public to seek out the detainees' side of the story.

But the court said the AP had produced no evidence that DoD responded differently to allegations of abuse depending on the nationalities or religions of the detainees. With no evidence of government impropriety in this regard, the court could not find that the public interest would be furthered based on a rationale grounded in disclosure of an individual's religion or nationality.

Because it found the balance clearly tipped in favor of privacy, the appeals panel said it need not squarely address the AP's "derivative use theory," namely that disclosure would eventually help the public understand the detainees' side of the story.

In Other Cases:

Judge Rosemary Collyer ruled that the **U.S. Army Corps of Engineers adequately searched** for and produced all relevant documents pertaining to the requester's property and his bid to get easement for a wetlands designation. "Mr. Short's speculation that the Army Corps maintains other documents in its records that were not released to him is insufficient to rebut the presumption of good faith accorded the Declarations of Mr. Francis and Mr. Lorenz," wrote Judge Collyer, noting that an agency's declarations are accorded "a presumption of good faith, which cannot be rebutted by purely speculative claims about the existence and discoverability of other documents." Citing various cases, she added: "An agency is not required to undertake a search that is so broad as to be unduly burdensome." (***Nation Magazine v. U.S. Customs Serv.***, 71 F.3d 885 D.C. Cir. 2003.) "It is the requester's responsibility to frame requests with sufficient particularity to ensure that searches are not unreasonably burdensome . . . [because] FOIA was not intended to reduce government agencies to full-time investigators on behalf of requesters." (***Judicial Watch, Inc. v. Export-Import Bank***, 108 F. Supp. 2d 19, D.D.C. 2000.) "Moreover, an agency is 'not obligated to look beyond the four corners of the request for leads to the location of responsive documents." (***Kowalczyk v. Dept. of Justice***, 73 F.3d 386, D.C. Cir. 1996). (***James R. Short v. U.S. Army Corps of Engineers***: USDC-D.C. – No. 07-2260 (RMC); Jan. 5.)

CIA Search

Judge James Robertson ruled the CIA adequately searched for documents concerning the CIA's *decision to initiate an internal review of the operations of the CIA's Inspector General*. The James Madison Project complained that the CIA did not produce at lease one of the IG's semi-annual reports. But Judge Robertson agreed with the CIA that "any documentation relating to the IG Office's compliance with the internal review would not be responsive to a request for records relating to the *decision to initiate the internal review* of the IG and the IG's office as a whole." He wrote, "The CIA's position rests upon a careful and literal, but not improper, reading of JMP's narrow and awkwardly worded FOIA request. The two Nelson declarations demonstrate that the search – for what JMP asked for – was reasonable." (***James Madison Project v. CIA***: USDC-D.C. – No. 08-0708; Jan. 6.)

E-Mails: DoT, EPA & OMB

In a 62-page ruling, Chief Magistrate Judge James Larson found that three agencies – DoT's National Highway Traffic Safety Administration, the Environmental Protection Agency and the Office of Management and Budget – properly withheld some e-mails and documents under Exemption 5. But he also found that other e-mails were purely transmittal in nature and must be disclosed, and that other documents contained factual data that must be segregated and released. The case was brought by the State of California. It involved the federal government's responses to

the State's regulations on motor vehicle carbon dioxide emissions. Judge Larson said the most helpful declaration was provided by Transportation Dept. (FOIA) Officer Kathy Ray. His recommendations must be adopted by the district judge. (***People of the State of California*** **v.** ***Environmental Protection Agency, et al.,***: USDC-N.D. Cal. – No. C 07-2055 JSW (JL)

Sierra Club v. USDA

In San Francisco, Senior Judge Samuel Conti ruled that Brazos Electric Power Cooperative could intervene in a FOIA suit brought by the Sierra Club. However, he declined Brazos' motion to transfer the case to federal court in west Texas. "Although the Sierra Club chapter that filed the FOIA request is headquartered in Austin, Texas, the Sierra Club's headquarters and the State in which it is incorporated is California. In addition, Sierra Club's principal place of business under § 552 is San Francisco. As the Ninth Circuit has recognized, a company incorporated in one State 'is not a resident [of another] for purposes of the venue statute.' According to this rule, Sierra Club is a 'resident' of California, not Texas. This is further reflected by the fact that the State of Texas legally recognizes the Lone Star Chapter of the Sierra Club as a 'foreign corporation,' incorporated in California and maintaining its principal place of business in San Francisco." (***Sierra Club v. U.S. Dept. of Agriculture, Rural Utility Services***: USDC-N.D. Calif. – No. 08-4248; Dec. 19.)

DHS Search

Judge Mark R. Kravitz ordered the Dept. of Homeland Security's FOIA Officer, Catrina Pavlik-Keenan, to supplement her declaration regarding the agency's search for records requested by Unidad Latina En Acción. "An agency cannot limit its search to only one record system if there are others that are likely to turn up the information requested. It is not clear from [the agency's] affidavit that the Central Records system is the *only* possible place that responsive records are likely to be located. *At the very least, [the agency] was required to explain in its affidavit that no other record system was likely to produce responsive documents*,'" he wrote, citing the D.C. Circuit's 1990 opinion in ***Oglesby v. U.S. Dep't of the Army***, (920 F.2d 57), "The Court believes it will be sufficient for Ms. Pavlik-Keenan to submit a supplemental declaration that states in reasonable detail: (1) where else, if anywhere, besides the Hartford DRO SDDO Operational File (Office of Detention and Removal Operations, Supervisory Detention and Deportation Officer) would the documents referred to in the Operational Order/Plan be maintained, if they had been created; (2) that DHS looked in those locations for those documents; and (3) that none of the documents was found. It may well be that DHS has already done each of these tasks, but regrettably, Ms. Pavlik-Keenan's Second Supplemental Declaration does not say so. Moreover, it is certainly possible that the documents in question would be maintained only in the Hartford DRO SDDO Operational File and nowhere else, and if so, Ms. Pavlik-Keenan can simply say so." (***Unidad Latina En Acción v. U.S. Dep't of Homeland Security*** : USDC-Connecticut – No. 3:07cv1224.)