PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Volume 26 Number 18, October 3, 2006

*CAPITAL INSIGHTS: The prospective chairmen of the House Financial Services Committee – both Republican and Democrat – predicted that legislation to beef up data security will not pass Congress this year. Rep. Spencer Bachus (R-AL), who is in line to chair the panel if the Republicans maintain their majority in the mid-term elections, and Rep. Barney Frank (D-MA), the Ranking Democrat, said there was not sufficient time left in this year's legislative session to reconcile the dozen different data-security bills pending in both the House and Senate. Speaking in Washington to the National Association of Federal Credit Unions, Bachus said that data security would be a top priority early next year, citing growing costs of data breaches to both consumers and banks. Frank also listed data security among his priorities . . . . Citing consumer complaints, Rep. Frank September 27 wrote to FTC Chairman Deborah Platt Majoras about the ongoing efforts of some major credit bureaus to steer consumers to Web sites where they pay for credit reports, rather than to the site created by the FACT Act where consumers can obtain their reports for free. The Frank letter also asks Majoras what can be done to make fraud alerts work better for consumers . . . . The U.S. Supreme Court has agreed to review a Fair Credit Reporting Act case (**Reynolds v. Hartford**) in which the Ninth Circuit U.S. Court of Appeals adopted what is viewed as a strong, pro-consumer standard for collecting punitive damages. Scott L. Nelson, an attorney at the Public Citizen Litigation Group, said that this time around, the move might not mean automatic reversal of another Ninth Circuit opinion. "The Ninth Circuit's view of the statute finds support in a number of Supreme Court opinions that treat reckless disregard of the law as equivalent to willfulness under various statutes," he wrote on the Public Citizen blog.* http://pubcit.typepad.com/clpblog/2006/09/supreme_court_t.html *. . . On Sept. 26, the House passed the Veterans Identity and Credit Security Act (HR 5835), imposing vigorous data security duties on the Dept. of Veterans Affairs. The measure would also afford data-breach victims free credit monitoring, free fraud resolution services and identity theft insurance up to $30,000. The bill now awaits Senate action.* *http://thomas.loc.gov/cgi-bin/query/D?c109:8:./temp/~c109QKX4wt::*

MAJOR STORIES IN THIS ISSUE

FOIA BILLS TARGET TIME LIMITS, FEES, BUSH MEMOS ROLE OF FOIA OFFICERS

Federal agencies should brace themselves: Congress appears serious about improving the workings of the Freedom of Information Act. On September 27, the House Government Reform Subcommittee unanimously approved legislation (H.R. 867) to strengthen the rights of FOIA requesters. The measures even address the role of FOIA/Privacy Act Officers.

The House bill seeks to enforce the Act's 20-day time limit, liberalize fee waivers, restore the "catalyst theory" for recovering attorney's fees, and override separate memos by ex-Attorney general John Ashcroft and White House Counsel Andrew Card that were seen as discouraging openness. It would also create a system to allow the public to track the status of FOIA requests online and via a telephone hotline. A Senate measure (S. 394) is similar, but would not override the Bush Administration memos.

Due the lack of remaining legislative days, most observers saw little chance that the bill would pass Congress. The House bill still awaits passage by the entire Government Reform Committee, and the Senate bill, approved by the Judiciary Committee, awaits floor action. Given Congress's overall workload, House and Senate Republican officials said no plans had been made to take up the FOIA bill during a weeklong session now scheduled between the Nov. 7 election and Thanksgiving. But Rick Blum, coordinator of the Sunshine in Government Initiative, said the recent action on bills will give "extra momentum" to the effort heading into next year.

Under the proposals, an agency would be required to give a "substantial" response within 20 days. If an agency did not comply, it would forfeit the right to withhold documents, unless they were protected by FOIA exemptions regarding national security, personal privacy or confidential business data, or their disclosure was otherwise prohibited by law. Blum said this provision attacks a practice by some agencies of simply acknowledging that they received a request.

In the House bill, an amendment by Ranking Democrat Rep. Henry Waxman (CA) would revoke the Ashcroft and Card memos. After the Sept. 11 attacks, then-Attorney General Ashcroft shifted from the Clinton administration's policy of "maximum responsible disclosure" to one emphasizing "institutional, commercial and personal privacy interests" when considering FOIA requests. In 2002, then-White House Chief of Staff Andrew Card's memo instructed agencies to "safeguard unclassified-but-sensitive" information, including data that could further development or use of weapons of mass destruction, or could be used "to harm the security of our nation."

Senate Judiciary Committee Ranking Democrat Patrick Leahy (VT) would be amenable to adding Waxman's Amendment to the Senate bill, his spokeswoman Tracy Schmaler said.

Both bills also call for a FOIA ombudsman to mediate disputes between the government and the public on information requests. Rep. Todd Platts (R-PA), who chairs the House subcommittee, said the proposed Office of Government Information Services, is central to the legislation. The office would be housed at the Administration Conference of the United States, which currently exists "only on paper," Platts said. The federally funded think tank was established in the 1960s to examine government management issues and functioned until 1995. It was reauthorized in 2004 but has yet to receive any funding.

"It is absolutely critical that there be a viable alternative to litigation," Platts said. Currently, if an agency denies a FOIA request, the petitioner "often has no option other than costly litigation in federal court," he said. The Administration Conference should be funded to fulfill that role, or lawmakers must find another entity to do the job, Platts said.

The amended House bill would require agencies to provide more details about time spent responding to FOIA requests, responsiveness to expedited review requests, and time spent on administrative appeals in annual reports. The bill directs the Office of Personnel Management, within a year, to submit a report to Congress examining: "whether changes to executive branch personnel policies could be made that would provide greater encouragement to all Federal employees to fulfill their duties under" the FOIA and Privacy Act."

The OPM report would also explore "enhancing the stature of officials administering" the Acts, and whether performance of compliance with the Acts should be included as a factor in personnel performance evaluations for any or all categories of Federal employees and officers. Finally, the study would examine whether an employment classification series for FOIA/Privacy Act officers should be established, and whether the highest level officials in particular agencies administering such sections should be paid at a rate of pay equal to or greater than a particular minimum rate. http://thomas.loc.gov/cgi-bin/query/D?c109:4:./temp/~c109fnqLYb::

CENSUS LEADS RECENT FEDERAL LIST OF LAPTOP LOSERS

The Census Bureau's admission that it lost hundreds of laptop computers with personal information had prompted a key house lawmaker to demand more details about the problem and to hold oversight hearings in October.

U.S. Rep. Mike Turner (R-OH), chairman of a House subcommittee on federalism and the census, told the *Dayton Daily News* he wanted a full accounting and detailing of lost devices by Oct. 12.

The Census Bureau announced in September that since 2003, there were 297 instances of potentially compromised personal data. These included: 217 laptops; 15 handheld devices; 46 thumbdrives; and the rest involved documents or other materials. The acknowledgement came in response to queries by House Committee on Government Reform Chairman Tom Davis (R-VA) to 17 agencies, of which 10 thus far have responded.

The Commerce Dept., of which the Census is a component, stood out. Altogether, 1,137 laptops had been stolen, lost or otherwise vanished since 2001, mostly from the Census Bureau and the National Oceanic and Atmospheric Administration. Of these, 249 contained personally identifiable information, nearly all from the Census Bureau. All were password-protected, a low-level safeguard. Only 107 of the computers were fully encrypted. Some lost laptops contained such personal information as names, incomes and Social Security numbers.

Commerce Secretary Carlos Gutierrez insisted "the vulnerability for data misuse is low," adding that the census computers require passwords and much information was believed to be encrypted. "We know of no instances of personal information being improperly used," he said.

Rep. Turner, however, said the Census Bureau has not investigated whether information has been compromised. "The Census Bureau needs to operate at a higher level of care," he said.

Gutierrez estimated that the disappearance of laptops from the Census Bureau could have compromised the personal information of about 6,200 households. The department was still trying to determine the extent of the problem, he said.

David Marin, staff director for the House Government Reform Committee, told the *Washington Post* that the failure of the remaining seven departments to respond to the queries could reflect their reluctance to reveal problems of similar magnitude.

HP SCANDAL SHINES LIGHT ON CORPORATE 'PRETEXTING'

The unfolding Hewlett-Packard pretexting-investigation scandal is supporting the view that intrusive, controversial techniques may not be uncommon in corporate investigations.

Patricia R. Dunn, the disgraced HP Chairwoman who resigned because of the scandal, defended before Congress her decision to investigate boardroom leaks, restating her position that it was necessary to protect company trade secrets and confidential deliberations.

"I believe that these methods may be quite common, not just at Hewlett Packard, but at companies around the country," she said of corporate-sponsored investigations. "Every company of consequence has people who do detective-type work in order to ferret out the sources of nefarious activities." HP launched its effort to flush out who leaked boardroom secrets after a series of news stories appeared in early 2005, citing sources close to its board. Investigators' actions, which members of a House Energy and Commerce subcommittee compared to B-grade movie scripts, have spawned both State and Federal criminal probes.

The *Boston Globe* reported that some of nation's the largest banks were customers of a Florida firm shut down this year for pretexting, or lying, to get personal information such as phone records, the same practice that HP admitted to.

The Florida case, involving banks such as Wells Fargo and Citigroup, isn't the only one in which large companies have been connected to practices like pretexting, but it is one of the most significant examples . It came to light in February, when Florida Attorney General Charlie Crist sued a Tampa-area company called Global Information Group Inc., claiming it made thousands of calls impersonating customers of companies including Verizon Communications Inc., tricking them into providing private call records . Earlier this year the company's principals agreed to pay $250,000 to settle the case, and to cease any pretexting activities. The deceit included impersonating a customer or employee, the case states. Verizon alone got more than 5,100 calls over a month from one Tampa-area phone number, and several other phone companies got thousands of calls. Global Information didn't admit to wrongdoing, and its attorney did not return The Globe's messages for this article.

When Global Information also was invited this year to testify at hearings held by the House Energy and Commerce Committee. Global Information's president, Laurie Misner, declined to

testify, citing her right against self-incrimination. But the company supplied documents to investigators, including a list of its largest customers for 2006. These customers included an auto-lending division of Wachovia, Wells Fargo, two units of Citigroup , and units of the Chase Bank division of J.P. Morgan Chase Co . The records don't say what each bank hired Global Information to do, but includes a column that appears to be the amount of money each spent on Global Information last year. The largest amount, $456,250.29, came from Wachovia's WFS unit, which specializes in auto lending, *The Globe* reported.

A spokesman for Wachovia said it ceased using Global Information Group this year and noted the bank's division that had employed the Florida company, WFS Financial, was independent before Wachovia bought it in February. A Wells Fargo spokesman said the bank's auto finance division ended its relationship with Global Information in November, for reasons he declined to discuss. Also, he said the bank has sent a memo to all its collections employees "making it clear that we do not permit 'pretexting.'"

A spokesman for Citigroup's CitiFinancial Auto lending group said in a statement it "has never sanctioned or condoned the use of pretexting, and after becoming aware of allegations that Global Information Group used pretexting methods, we terminated our relationship with them in November 2005. We also instructed all other similarly engaged vendors that they are forbidden to use pretexting on our behalf." A spokesman for Chase Bank declined to comment, *The Globe* said.

All four national banks are regulated by agencies including the Office of the Comptroller of the Currency and the Federal Reserve. A comptroller's spokesman said the agency had no information about national banks involved in pretexting but added that it does not oversee at least four of the bank divisions that appeared on Global Information's list. A Fed spokesman said the agency couldn't discuss the matter. Mierzwinski and other consumer advocates once praised the comptroller's office in particular for being in the forefront of identity theft issues, such as a 2001 notice in which it told banks they should not "use the services of anyone the bank suspects may be engaging in pretexting to obtain customer information." But Mierzwinski and others, including Gail Hillebrand of Consumers Union, say the agency lacks resources to follow up on all its guidance from the past. Rep. Edward J. Markey (D-MA), who sits on the House Energy and Commerce Committee, sent a letter this week to the comptroller asking what action the office has taken to follow up on the Florida case.

GARTNER: CHOICEPOINT SPENT $30 MILLION TO IMPROVE SECURITY, 'CREDENTIALING'

Since 2005, when ChoicePoint became the "Poster Child" for security breaches and privacy invasions, the company has spent nearly $30 million on improvements in employees, training, technology and "credentialing" to ensure customers are for real, according to the Gartner , a well-known business consulting firm.

Authored by analyst Avivah Litan, the study asserts that ChoicePoint has transformed itself into "a role model for data security and privacy practices." Unfortunately, the study does not address some key privacy issues associated with the company, or potential costs that still might arise from the 2005 data breaches.

ChoicePoint hit the headlines in 2005 after a ring of Nigerian fraud artists posed as legitimate businesses to gain access to the company's rich trove of personal data. The fraudulent access continued for months, with the records of some 145,000 individuals wrongly compromised, and about 800 confirmed victims of identity theft.

Following an investigation by the Federal Trade Commission (FTC), ChoicePoint agreed in January 2006 to pay a $10 million fine and to spend $5 million for consumer redress. In addition, the company agreed to an injunction for up to 20 years for some provisions, stating that it had to: (1) "Credential" its customers that are regulated by the Fair Credit Reporting Act (FCRA); (2) inspect certain of its customers' facilities; and (3) conduct independent audits and submit to extensive monitoring by and reporting to the FTC.

Accordingly, ChoicePoint first move came on the "corporate governance" front, creating a Chief Credentialing, Compliance and Privacy Officer (CCCPO), who reported to the Privacy and Public Responsibility Committee of the company's board of directors. It named Carol A. DiBattiste a former federal prosecutor and executive with the U.S. Department of Justice, as CCCPO. (On September 28, it promoted DiBattiste to general counsel and chief privacy officer.)

Considerable attention went into credentialing – that is, ensuring that customers were legitimate businesses, not fraudsters. Gartner said that ChoicePoint lost $20 million in revenues because it refused to sell to businesses that could not be credentialed.

In the third quarter of 2006, ChoicePoint rolled out a mandatory online privacy training program for all permanent and temporary employees and independent contractors who research court records. A second information security awareness program was also recently introduced. Employees are now tested annually for successful completion of both programs and must score at least 80%. In August 2006, ChoicePoint also rolled out social engineering training programs for call center employees so that they would not fall victim to fraudsters' phone tricks.

Auditing was also stepped up. It became one of the most-audited companies in the U.S. in 2005, undergoing 43 third-party audits. In 2006, ChoicePoint said it expected to complete up to 30 audits, including an extensive one required by the FTC.

"The company took advantage of a crisis to make fundamental changes to conduct its business more securely. New data security projects were driven and sponsored by ChoicePoint's chairman, president and the board (notwithstanding the FTC order, and the fact that its survival depended on it," Litan wrote in the Gartner study. "The entire company became involved in understanding, implementing and ensuring compliance with the new privacy and security agenda. The process was not restricted to only a few divisions."

Among the "lessons learned," Litan listed,

- Business transparency is critical, especially when you are a custodian of confidential consumer data.

- Credentialing customers involves many nuances, and credentialing most smaller, unknown business customers with little transaction history is generally not worth the effort or the cost. The market lacks standards in customer credentialing.

- Audit, compliance and training are critical tools to ensure people and organizations follow through on stated objectives and practices.

- Considerably more work is required to change the business culture and practices than to implement security technology applications.

Chris Hoofnagle, a senior staff attorney to the Samuelson Law Policy Clinic at the University of California-Berkeley Boalt Hall School of Law, said the report accurately described how ChoicePoint had moved more quickly to comply with security safeguards than some of its counterparts, including LexisNexis and Acxiom.

CHINESE SCRIBE PLANS TO SUE YAHOO BRANCH OVER PRIVACY

A jailed Chinese journalist plans to file a lawsuit against Yahoo because one of its subsidiaries gave his e-mails to the Chinese government, according to the journalist's lawyer.

Shi Tao, the dissident journalist, was convicted of "divulging state secrets" and sentenced to 10 years in prison after Yahoo Holdings (Hong Kong) provided his e-mails to the Chinese government. Shi's e-mail, sent from a Yahoo account in April, 2004 to a pro-China democracy Web site in New York, contained a Beijing order for officials to be on guard for unrest and dissident activity ahead of the 15th anniversary of the Tiananmen Square massacre.

Albert Ho, a legislator in Hong Kong and Shi's lawyer in the case, told IDG News Services that the suit will likely be filed in either New York or California in the next few months. He said Shi, who is not a U.S. citizen, could file a lawsuit in the country under the Alien Tort Claims Act of 1789. The group has not yet decided on a U.S. law firm to retain for the case, nor would Ho divulge the specific strategy or damages the group intends to seek.

"We're also trying to line up other victims for a class-action. We've been in touch with a few others, but we haven't signed anyone up yet. It's a very sensitive issue because there could be reprisals against their families," said Albert Ho

The new lawsuit would come just months after Ho filed a complaint with Hong Kong's Office of the Privacy Commissioner for Personal Data against Yahoo Holdings (Hong Kong) on behalf of Shi. The case is pending. Yahoo could face a fine, a civil lawsuit, or both if the Privacy Commissioner finds that it illegally divulged personal data used to put Shi in jail. The plaintiffs argued that Yahoo Hong Kong had no right to comply with a request from China for Shi's personal data, and requested that the office investigate the matter.

Yahoo has denied any involvement in the case by its Hong Kong arm. The company has said any information provided to Chinese authorities in this case would have come from Yahoo's operations in China, rather than Hong Kong. However, Yahoo's Chinese and Hong Kong operations were both part of the same corporate entity, Yahoo Hong Kong, at that time In 2005, Alibaba.com acquired Yahoo's Chinese operations as part of a deal that saw Yahoo take a stake in the Chinese Internet company.

International pressure is increasing on Internet companies to handle their users' private data more carefully, particularly with respect to human rights. Amnesty International and Reporters Without Borders have both criticized Yahoo over the Shi incident, and a group of U.S. lawmakers blasted a group of Internet companies earlier this year, including Yahoo, Google, Microsoft, and Cisco Systems, for failing to uphold free expression in China. Yahoo had no comment, the news service reported.

FOIA CT. ROUNDUP: GUANTANOMO IDs; WACHOVIA'S SUBPRIME LENDERS

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

Associated Press v. U.S. Dept. of Defense: (No. 05-5468 PLF)
Court: U.S. District Court for the Southern District of New York
Judge: Jed S. Rakoff
Exemptions: FOIA (b)(6) & (7)(C), privacy; & (b)(1), national security, (b)(5)
Documents: Identities of detainees at Guantanomo Bay detention center
Issues: Privacy for detainees allegedly subjected to abuse?
Date: September 20, 2006

In another potentially groundbreaking decision, the court ordered the Defense Dept. to disclose to the Associated Press nearly all of the identities of detainees at Guantanomo Bay who were allegedly victims of abuse at the hands of U.S. officials. The decision confirmed that there has been at least eight DoD investigations of alleged abuse of detainees by U.S. officials at Guantanomo Bay.

"There must be weighed against the detainees' minimal privacy interest purportedly here asserted on their behalf by their captors the considerable public interest in learning more about DoD's treatment of identifiable detainees, whether they have been abused, and whether such abuse has been properly investigated," wrote Judge Jed S. Rakoff.

Citing the U.S. Supreme Court's FOIA opinion in ***Favish***, Judge Rakoff said that to overcome the privacy exemption, a requester must produce evidence of government impropriety.

"Here, AP has certainly made such a showing. In addition to the public allegations of certain detainees described above, certain military offices and FBI agents who have worked at Guantanomo have also questioned the treatment of detainees."

"By redacting the identities of the abused detainees, DoD has seriously interfered with the ability of the public to engage in the independent fact-finding necessary to properly evaluate the allegations of abuse and DoD's response to it," he wrote.

Judge Rakoff found that it was illogical to believe that privacy was a priority for detainees. "But the records here concern, almost entirely, the behavior of the agency and its employees, not that of the detainees, and it appears that even the redacted medical records were concerned, not with the detainees' pre-existing medical conditions or treatments, but with the medical evidence of *vel non* of the abuse they allegedly suffered."

"Although revelation of abuse by one's captors may cause some limited embarrassment, most people in such situations – especially individuals detained incommunicado without many procedural safeguards – would want their plights and identities publicized," he continued.

"Indeed, three former detainees issued a 115-page report in 2004 alleging they were beaten and otherwise mistreated while at Guantanomo. Moreover, many current detainees have participated in hunger strikes to protest alleged abuse. In all such instances, the detainees have not hesitated to reveal their identities," he wrote.

For a detainee to be released, an Administrative Review Board must recommend release to a Designated Civilian Official (DCO). The DCO then decides whether the detainee should be released, transferred or remain at Guantanomo.

Judge Rakoff rejected Exemption 5 protection for DCO decisions, finding they were not predecisional or deliberative, but were, in fact, final decisions.

While acknowledging that Exemption 5 can extend to other privileges, he also dismissed DoD's claims that disclosure would interfere with its ability to transfer wartime detainees and conduct diplomatic relations.

"DoD's own language shows that DoD is surreptitiously seeking to invoke FOIA Exemption 1 – the so-called national security exemption – under the cover of Exemption 5, even though the Government has previously disclaimed any reliance on Exemption 1 in this case. The Government cannot have it both ways," he wrote.

Inner City Press/Community on the Move v. Bd. Of Governors, Fed. Reserve: (No. 05-6161)

Court: U.S. Court of Appeals for the Second Circuit
Judges: Restani, Miner & Calabresi
Exemptions: FOIA (b)(4), confidential business data
Documents: Wachovia Corp.'s relationship with subprime lenders
Issue: When is information considered to be in the public domain?
Date: September 11, 2006

The appeals panel reversed part of a decision that would have required the Federal Reserve Board (Fed) to disclose the names of subprime lenders with which Wachovia did business. Wachovia had submitted the information to the Fed as part of its application to merge with SouthTrust Bank.

The three-member panel of the Second Circuit (New York) found that the information was submitted voluntarily, and was protected as confidential under Exemption 4 because disclosure would impair the government's ability to collect it in the future. Thus, the information would only have to be disclosed if it were deemed to be in the "public domain."

The district court agreed with requester Inner City Press (ICP) that the information was publicly available through Wachovia's filings with the Securities and Exchange Commission. But the appeals panel held that ICP did not meet its "burden of production," because the SEC forms it cited contained different information than what was being requested in this case.

"[SEC] Form S-1 reveals the identity of a registrant's *principal* underwriters, not *general* underwriters. ICP has not shown that Exhibit 3 contains information that Wachovia was a principal underwriter to some of its subprime-lending clients," wrote Judge Jane Restani. The panel remanded the case to the district court to determine if ICP could meet its burden of production. However, the appeals panel rejected the Fed's argument that information in SEC databases was not "freely" available to the public, just as the Supreme Court found that "rap sheets" and other criminal records were not freely available in ***Reporters Committee***.

"Securities filings also do not have the same privacy concerns as criminal records. While government agencies assemble rap sheets for their own use and limit their disclosure due to privacy concerns, the SEC collects securities filings and makes them available to the public. Moreover, the goal of securities filings themselves is to protect investors by requiring full disclosure of material information. Therefore, the ready availability of securities filings and the policy favoring disclosure of information found in securities filings distinguishes this case from ***Reporters Committee***," Judge Restani wrote.

IN BRIEF . . .

President Bush's Identity Theft Task Force, headed by Attorney General Alberto Gonzales and FTC Chairman Deborah Platt Majoras, has issued its "interim recommendations for Administration action, including: (1) that the Office of Management and Budget (OMB) issue agency guidance on responses to data breaches, notification and mitigation of identity theft risks; (2) development of a universal police report for identity theft victims; (3) extending restitution for ID theft victims; (4) reducing access of ID thieves to Social Security Numbers; (4) developing alternative methods of "authenticating" IDs; (5) improving data security in government, and improving agencies' ability to respond to data breaches. The task force recommended that OMB and the Department of Homeland Security (DHS) take the lead on the latter issue.
www.ftc.gov/os/2006/09/060916interimrecommend.pdf & www.usdoj.gov/opa/pr/2006/September/06_ag_636.html