

**INFO TECHNOLOGY**

## Google, China in Internet Scuffle

**G**oogle may leave China, the biggest Internet market in the world,

after a December cyber attack on its network that resulted in theft of its intellectual property.

The search engine giant said it would stop filtering content on its Chinese language *Google.cn* engine as required by the Chinese government and would try to negotiate a legal unfiltered search engine. If not, Google may leave the market, *Reuters.com* reported. The Chinese government told its local media that all foreign companies, including Google, must follow Chinese laws that require Internet firms to filter content.

China has about 384 million Internet users, media reports said, and they are mostly restricted from

viewing online information the government deems incendiary or threatening, including the June 4, 1989, Tiananmen incident. In China, search requests that include words like “Tiananmen Square massacre” or “Dalai Lama” come up blank.

In recent months, *The New York Times* said, the government has also blocked Google’s YouTube service. Last summer, the government briefly blocked access nationwide to Google’s main search engine and other services like Gmail. It also forced the company to disable a function that lets the search engine suggest terms, arguing that it was trying to remove

pornography from Google’s search engine results.

The U.S. government has expressed its support for Google and sent a diplomatic note to China formally requesting an explanation for the attacks, according to *Reuters.com*. It has long been concerned about Beijing’s cyber-spying program, which a congressional advisory panel said appears to be illegally accessing U.S. computers in an attempt to steal data for nefarious purposes. Canadian researchers recently discovered that computer systems based in China had stolen online digital documents from hundreds of government and private organizations worldwide.

Google entered the Chinese Internet space in 2006 and quickly became the number two search engine, behind local competitor Baidu, which reportedly has a close relationship with the Chinese government, says *Reuters.com*. Google has been criticized by the Western world because it agreed to self-censor searches as required by the Chinese government. Chinese authorities have denied they censor the Internet.

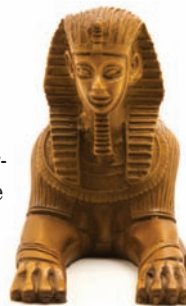
The sophisticated cyber attacks that recently hit Google’s computer systems were aimed at the Gmail user accounts of Chinese human rights activists, *The Times* reported, in addition to 34 companies or entities, mostly located in the Silicon Valley area. The attackers may have succeeded in penetrating elaborate computer security systems and obtaining crucial corporate data and software source codes. Google said these attacks, combined with increased curbs on free speech on the Web, had led to the review of its business in China.

**ARCHIVES**

## Egyptian Archives Go Digital

**T**he world now can access part of Egypt’s cultural heritage online. The digital documentation of the National Archives of Egypt (NAE) is now one of the largest digital archives in the world, with more than 25 million records containing more than 90 million documents.

The national project, which is based on a state-of-the-art solution from IBM, includes a website ([www.nationalarchives.gov.eg/nae/home.jsp](http://www.nationalarchives.gov.eg/nae/home.jsp)) providing online access to a selection of the archived material.





## PRIVACY

### Report: FBI Lied to Obtain Phone Records

Between 2002 and 2006, the Federal Bureau of Investigation (FBI) made up terrorism emergencies to illegally collect more than 2,000 phone records from phone companies, according to a report from the Department of Justice (DOJ).

The 289-page report revealed how FBI officials violated their own procedures meant to protect civil liberties and strained their communication analysis unit with non-emergency requests. In many cases, the FBI issued approvals after the records had been collected to justify its actions, the report found.

In an interview with *The Washington Post*, FBI General Counsel Valerie Caproni admitted the bureau violated the Electronic Communications Privacy Act in collecting the 2,000 phone records.

IDG News Service said the agency used simple verbal requests and even Post-It Notes to request customer records from telecom providers. In many cases, FBI agents said they had secured the required authority to make such requests when they had not. Even when the FBI used formal

written requests, it did not track their use or keep copies of them, according to the report.

According to IDG, the report also found the FBI obtained phone records about reporters working for *The Washington Post* and *The New York Times* without complying with relevant laws. FBI Director Robert Mueller did not become aware of these problems until late 2006 or early 2007 when they were discovered by an inspector general investigation, according to the Associated Press.

In its defense, the FBI said agents were working to stop potential terrorist threats and did not intentionally break the law. Bureau officials said nearly all the instances of illegally collecting phone records were related to terrorism cases. The FBI also said it has taken steps to ensure this will not happen again and has destroyed records obtained illegally. According to *Network World*, after 2007, the DOJ report noted, the agency made serious changes that have helped prevent illegal access to phone records, although the report recommended additional action to ensure the problem does not continue.

The Electronic Frontier Foundation has filed a lawsuit against the government and said the violations revealed in the DOJ document have not been disclosed by the FBI during the course of the ongoing lawsuit.

## LEGISLATION

### REAL ID Deadline Extended Again

The Department of Homeland Security (DHS) says the May 10, 2011, deadline for full compliance with the REAL ID Act is still in effect, despite the fact that many states have not met past deadlines, which has forced DHS to extend deadlines repeatedly. The REAL ID Act's purpose is to implement national standards for driver's license and identification documents to enhance security and reduce fraud. Only identification in compliance with REAL ID is to be accepted for federal purposes, such as proving identity to board airline flights.

According to a December 18, 2009, statement from DHS, 46 of 56 states and territories were not expected to be able to meet the December 31, 2009, deadline to be in full compliance with REAL ID. That deadline was extended to May 10, 2011, and DHS said it would work with states to meet this new deadline. However, it said Congress must fix systemic problems with the REAL ID Act to advance U.S. security interests over the long term.



## E-MAIL

## White House Settles Missing E-Mail Suits



Citizens for Responsibility and Ethics in Washington (CREW) and the National Security Archive (NSA) settled their lawsuits criticizing the George W. Bush White House and the National Archives and Records Administration (NARA) for failing to act after learning that millions of e-mails had gone missing from White House servers during a two-and-a-half-year period. CREW is a non-profit organization dedicated to promoting ethics and accountability in government; the NSA is an independent research institute and library located at The George Washington University.

According to CREW's lawsuit, the White House had discovered the problem in the fall of 2005 but failed to recover or restore the missing e-mails. In addition, the White House knowingly continued to use a broken system for preserving e-records.

*ComputerWorld* reported that the problems began after the White House moved from Lotus Notes to Microsoft Exchange. At the same time, Bush's IT staff also stopped using the electronic management and archiving system called Automated Records Management Systems, which was put in place in 1994. Development began on a new archiving system, but there were problems and it

was never implemented, according to *ComputerWorld*. As a result, the White House was left with manual processes to archive e-mails, which led to mislabeled and unorganized files.

Under the terms of the recent settlement, *ComputerWorld* reports that the Executive Office of the President (EOP) will restore a total of 94 days of missing e-mails, which it will send to NARA for preservation and eventual access under the Presidential Records Act or the Federal Records Act. The dates for restoration were chosen based on e-mail volume and external events, as it was too expensive to restore all the missing e-mails. According to *ComputerWorld*, nearly 22 million Bush e-mails have been recovered to date.

In addition, the EOP will continue to provide CREW and the NSA with records documenting the missing e-mail problem, the response of the Bush White House, and the options for preserving e-records the Bush White House considered but ultimately rejected. To date, the Obama White House has produced thousands of pages of documents relating to these issues. CREW has posted them at [www.governmentdocs.org](http://www.governmentdocs.org).

Finally, the settlement requires the EOP to release a description of the system it now uses to manage

and preserve e-records, including its e-mail archiving and backup systems. According to the NSA, the EOP's letter in January announced the features of its system:

- Captures and preserves all e-mail and Blackberry messages sent or received on the EOP's unclassified network
- Divides documents into component-specific repositories and broad search capabilities that improve the ability to find e-mail records in response to legal or administrative needs
- Blocks access to personal and external web-based e-mail systems from White House unclassified workstations
- Controls against unauthorized deletion of e-mails and provides an accounting of any deleted e-mails
- Consists of systematic emergency recovery backups of the system
- Generates audit reports and system health-check dashboard reports to help identify problems

Experts say the new system automatically accounts for the capture, backup, and preservation of e-mails – all of which were missing in the previous administration's system. According to Kristen Lejnieks, NSA counsel, the new system includes controls and automated reporting that will quickly bring unauthorized actions to light for investigation.

According to *The Washington Post*, many of the newly restored e-mails may not be made public. Any restored e-mails will become part of NARA's Bush collection, and officials said many will probably be withheld for security reasons or because they are considered presidential records exempt from the Freedom of Information Act. Bush's presidential records that are released will not be available until 2014 at the earliest.

**PRIVACY**

## Supreme Court to Rule on Employee Privacy

All employees who e-mail or text using a company-owned device or system will want to pay close attention to how the U.S. Supreme Court rules in the landmark case *Ontario v. Quon*.

The court will review the case this spring and determine whether government employees specifically have a reasonable expectation of privacy when e-mailing or texting using company-owned systems. However, the ruling is also expected to affect private sector employees and employers' formal and informal policies regarding electronic communications.

At issue is whether the Ontario (Calif.) Police Department violated an officer's constitutional right to privacy when it reviewed personal

for text messaging, however.

Each pager user was given a monthly limit of 25,000 text characters. Under an informal policy put in place by a police lieutenant, as reported by *The Washington Post*, officers who exceeded the limit were required to pay overage charges if they did not want their pager to be audited. Sgt. Jeff Quon and others regularly exceeded the limit and paid the charges.

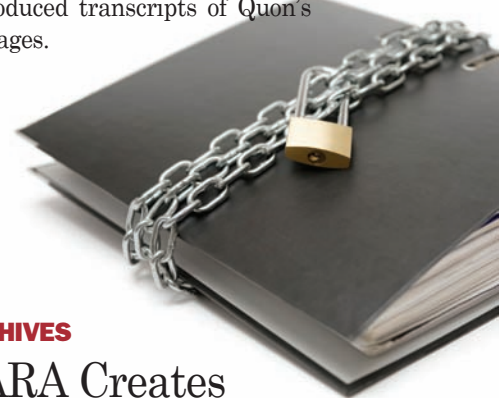
When the department decided to review pager usage to determine whether to increase the character limit, it discovered only 57 of more than 450 messages sent and received by Quon involved police business. Many of the others were sexually explicit private messages. The department ordered transcripts of the messages from Arch Wireless, the city's text messaging provider.

Quon and three others sued the city of Ontario in 2004, claiming their Fourth Amendment rights against unreasonable searches and seizures had been violated. They believed the informal policy created a reasonable expectation of privacy for their personal messages.

The police department argued there should have been no such expectation and that the lieutenant's billing practice was not an official policy. The League of California Cities and the California State Association of Counties filed friends of the court briefs pointing out the police department's "operational realities" made an expectation of privacy unreasonable and the text messages could be subject to public information requests under the California Public Records Act.

Nevertheless, the Ninth Circuit Court of Appeals in San Francisco found in favor of Quon, ruling the city could have told him about the text message review and given him

a chance to redact his personal messages. The court said the chief's decision to read the messages without a suspicion of wrongdoing by Quon violated his Fourth Amendment protections against unreasonable searches. In addition, the court ruled Arch Wireless violated the Stored Communications Act when it produced transcripts of Quon's messages.



**ARCHIVES**

## NARA Creates Holdings Protection Program

U.S. Archivist David S. Ferriero announced the creation of the National Archives and Records Administration (NARA) Holdings Protection Program and the appointment of key team members.

In making the announcement, Ferriero said, "The issue of collections security is one of my highest priorities. We absolutely must be able to ensure that the National Archives is able to safeguard the documentary heritage of our nation. This new initiative will help us achieve that goal."

The Holdings Protection Program will serve as a nationwide resource, developing and administering policies to enhance holdings protection of original records, regardless of their format, to reduce the loss of and aid in the recovery of holdings while ensuring ready access for research by all stakeholders. The team will work with individual offices within NARA in Washington, D.C., the regional archives and records centers, and the 13 presidential libraries.



text messages sent and received on a government-issued pager. When the department issued pagers to officers, it had a formal policy covering computer, Internet, and e-mail usage stating the systems were for official use only. The policy allowed for "light personal communications" but warned employees should have no expectation of privacy. There was no specific policy



**LEGISLATION****Bye, Bye, SOX?**

**T**he Sarbanes-Oxley Act (SOX) may be declared by upcoming U.S. Congress and Supreme Court decisions.

The House of Representatives recently voted to approve the Garrett-Adler amendment, which would exempt small companies from SOX Section 404 provisions, while the Supreme Court is considering the constitutionality of the Public Company Accounting Oversight Board (PCAOB).

These developments may have long-term implications for SOX, the 2002 legislation passed in the wake of the Enron, WorldCom, and Tyco scandals. The outcomes may also have implications for records managers, information technology specialists, and compliance officers who devise and implement company controls.

Section 404 of SOX requires company auditors to attest to the soundness of the firm's internal controls and financial statements. Internal controls may include anything from transaction approval authorizations to records retention programs. This provision is widely blamed for an increase in auditors' fees, as well as increased expenditures to ensure that proper internal controls are in place.

Small firms – those with less than \$75 million in market capi-

talization – have protested that compliance with SOX 404 would cost them a disproportionate share of their earnings. The complaint is supported by an independent study conducted at Pennsylvania State University, which showed that firms just over the \$75 million mark paid nearly \$700,000 more in audit fees and had average earnings of negative \$1.4 million in 2004.

The deadline for small firm SOX compliance has been extended four times, but they won't need to comply at all if the Garrett-Adler amendment makes it to the Senate floor as a standalone bill.

SOX also established the PCAOB to oversee and regulate audit firms. PCAOB operates under the supervision of the Securities and Exchange Commission (SEC), which also appoints PCAOB members. It is funded by fees charged to audited firms. When it was established, Congress wanted the board to be separate, with its own funding stream, and outside normal civil service laws so it could attract highly qualified specialists. PCAOB members' salaries are more than \$500,000 and are reviewed by the SEC.

Pro-business advocates, represented by the Free Enterprise Fund, argue that the PCAOB's governance structure is unconstitutional because it is an independent agency that does not allow for the president to appoint members. Additionally, because only the president can remove SEC commissioners for cause, and because the SEC can only remove PCAOB members for cause, some court members believe this is a formerly unrecognized limit of the president's powers that may contradict the constitution.

The Supreme Court will take up the issue soon, and some legal experts believe that SOX could be abolished completely if the court rules the PCAOB unconstitutional.

**ARCHIVES****President Approves \$470 Million for NARA**

**T**he National Archives and Records Administration (NARA) received a Fiscal Year 2010 budget of \$469.87 million under the Consolidated Appropriations Act signed by President Barack Obama on December 16, 2009.

This represents an increase of 2.31% over last year's funding of \$459.27 million. For NARA's FY2010 operating expenses, the president and Congress have provided \$339.77 million, an increase from last year's appropriation of \$330.30 million.

For continued development of the Electronic Records Archives (ERA), Congress appropriated \$85.5 million, up from last year's \$67 million. For repairs and renovations at NARA-owned facilities, lawmakers appropriated \$27.5 million. This includes \$17.5 million that is the last installment for repairs and renovations at the Franklin D. Roosevelt Presidential Library in Hyde Park, N.Y. The Roosevelt Library is the oldest of the 13 presidential libraries administered by NARA.

The National Historical Publications and Records Commission, the grant-making arm of NARA, will receive \$13 million, up from last year's \$11.25 million. In addition, \$4.5 million will go toward providing online access to the papers of the Founding Fathers.



**E-DISCOVERY****Scheidlin Revisits  
Zubulake**

Six years after her e-discovery ruling in *Zubulake v. UBS Warburg*, U.S. District Judge Shira Scheindlin has revisited and revised that landmark decision in her ruling in another case.

In *Zubulake*, Scheindlin ruled that failing to preserve backup documents during discovery could be considered gross negligence. In a recent case, *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities LLC*, the federal judge imposed sanctions on 13 investors for deleting e-mails and destroying records in their lawsuit over the collapse of two hedge funds.

In 2004, 96 investors filed a lawsuit to try to recoup \$550 million after two British Virgin Islands-based hedge funds failed and were liquidated. They accused the funds' former directors, administrators,

auditor, and the prime broker and custodian of securities violations. One of those entities named in the lawsuit, Citco Fund Services, was hired as administrator but resigned, according to *Courthouse News Services*.

During discovery, Citco accused the plaintiffs of not producing all relevant documents. Citco requested the case be dismissed, but Scheindlin said she could not find ample evidence of blatant misconduct on the part of the plaintiffs.

However, the federal judge did agree with Citco that the missing documents were relevant to the litigation and that the investors failed to preserve key electronic records. Thirteen of the shareholders "continued to delete electronic documents after the duty to preserve arose, did not request documents for key players, delegated such ef-

orts without any supervision from management, destroyed backup data potentially containing responsive documents of key players, and submitted misleading or inaccurate declarations," her ruling states.

The judge instructed the jury to presume that all missing evidence was favorable to the Citco defendants. She imposed monetary sanctions, including attorney fees, against all 13 investors for being negligent and grossly negligent in the preservation and collection of electronic documents pertinent to the case.

"While litigants are not required to execute document productions with absolute precision, at a minimum they must act diligently and search thoroughly at the time they reasonably anticipate litigation," Scheindlin wrote in her statement. "All of the plaintiffs in this motion failed to do so and have been sanctioned accordingly."

The ruling means, according to *Courthousenews.com*, that Citco will be compensated for costs and attorney's fees, including fees and expenses associated with filing sanctions motions, reviewing declarations, and deposing declarants. As *IM* goes to press, the amount has not yet been determined.

In her opinion, Scheindlin noted that she and her two law clerks wasted nearly 300 hours resolving the motion. She also wrote that, six years after the court's groundbreaking *Zubulake* opinions, and decades after courts first addressed electronic discovery, litigants are still conducting e-discovery in an "ignorant and indifferent fashion," *Law.com* reported. She advised parties to "anticipate and undertake document preservation with the most serious and thorough care," if for no other reason than to avoid sanctions.

**PRIVACY****Microsoft to Reduce EU Data Retention**

After years of fighting European Union (EU) privacy regulators, Microsoft Corp. has agreed to delete the Internet protocol addresses of EU users after six months.

Previously, Microsoft held search records for 18 months. The new policy will be implemented over the next year to 18 months, according to a public announcement by John Vassallo, Microsoft's vice president of EU affairs.

EU officials have been convinced for years that Microsoft was breaching its strict privacy laws by retaining user data for such a lengthy amount of time. In October 2009, EU officials told Microsoft, Google, and Yahoo! to limit the amount of time they retain Internet-search records to six months or less, in accordance with the EU's data protection laws.

Yahoo! has cut its data retention period to only 90 days. Google Inc. still retains data for nine months, but it may feel pressure to reassess its retention policy.



## HEALTH RECORDS

### Breaches Affected 50% of Hospitals in 2009

A new survey reveals that business associates who handle private patient information for healthcare organizations – including billing, credit bureaus, legal services, claims processing, insurance brokers, data processing firms, pharmacy chains, and offshore transcription vendors – are not ready to meet the new data breach-related obligations included in the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Healthcare Information and Management Systems Society (HIMSS) analytics national survey of hospitals and business associates revealed that about one-third of business associates surveyed were not aware that they need to follow federal Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements.

Of the hospitals and health providers surveyed, 85% said they would take steps to ensure that data held by business associates will not be breached. Nearly half of hospitals (47%) said they would actually terminate their contracts with their business associates for violations.

The survey also found that:

- Of large hospitals, 50% experienced at least one data breach in 2009.
- Of all hospitals, 68% indicated the HITECH Act's ex-

panded breach notification requirements will result in the discovery and reporting of more incidents.

- Of all hospitals, 57% reported they now have a greater level of awareness of data breaches and breach risk.
- Of hospitals, 90% have changed or plan to change policies and procedures to prevent and detect data breaches.

Businesses that suffer data breaches will likely pay dearly for it in the future. The U.S. Department of Health and Human Services (HHS) recently issued an interim final rule addressing its enforcement of HIPAA. The HITECH Act, which was enacted as part of the American Recovery and Reinvestment Act of 2009, greatly increased the penalty amounts the HHS secretary can impose for HIPAA violations occurring after February 18, 2009.

Prior to the HITECH Act, the secretary could not fine violators more than \$100 for each violation or \$25,000 for all identical violations of the same provision. A covered healthcare provider, health plan, or clearinghouse could also bar the secretary's imposition of a civil money penalty by demonstrating that it did not know it violated the HIPAA rules. Section 13410(d) of the HITECH Act strengthened the civil money penalty scheme by establishing tiered ranges

of increasing minimum penalty amounts, with a maximum penalty of \$1.5 million for all violations of an identical provision. In addition, a covered entity, which includes business associates, can no longer plead innocence because of ignorance of the breach unless it corrects the violation within 30 days of discovery.

## INFO TECHNOLOGY

### More Government Data to the Cloud?

According to a recent report, the U.S. government spent \$277 million on cloud computing in 2008, and that amount will increase to \$792 million by 2013.

The report, *Moving to the Cloud: An Introduction to Cloud Computing in Government*, by Southeastern Louisiana University professor David Wyld, explains that while NARA received 200 million e-mails from the outgoing Bush administration, the Obama administration could generate more than 1 billion e-mails, thus the need for cloud computing.

There are many definitions of "cloud computing," but Wyld's report used the National Institute of Standards and Technology definition: "a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."



**GOVERNMENT RECORDS**

## Another Delay for FBI's Sentinel System

**T**he Federal Bureau of Investigation's (FBI) \$451 million case management system, coined the "Sentinel," has been delayed yet again. According to media reports, the full deployment of the system, which will be used to search and analyze criminal and national security data, has been pushed back to September 2010.

The case management system was started in 2005 and is being developed by Lockheed Martin. It is expected to replace the FBI's largely paper-based operation with a single digital system. In November 2007, the FBI extended the completion date from December 2009 to June 2010, *InformationWeek* reported. The latest delay was reported in an audit by the FBI's inspector general.

Sentinel is supposed to replace the agency's web-based Virtual Case File program, which was scrapped after the FBI spent \$170 million on the program. Despite the delays, Sentinel won't be a similar disappointment, according to the Government Accountability Office, which has recommended the system as a model for the rest of the FBI, *InformationWeek* said.

The agency is rolling out Sentinel in phases. The first phase, completed in June 2007, of-

ferred a new user interface and improved searches for case information already in its databases, as well as work boxes that summarize cases and leads.

During the second phase, which was scheduled to be completed in July 2009, the FBI and Lockheed encountered problems developing forms and document workflows. Phase two ended months behind schedule and \$18 million over budget, delaying the completion date. The inspector general reports that phase two capabilities, including a new

portal, electronic forms, migration of FBI case records to a new system, and an automated document and case file workflow management, just recently became available to users, *InformationWeek* said.

In the final phases of Sentinel's development and deployment, the FBI plans to migrate case data from an antiquated case management system to Sentinel, connect Sentinel to other FBI systems, increase access controls, and add forms to Sentinel's electronic form library.

Past due

**ARCHIVES**

## NARA to Study Haldeman Notes

**T**he National Archives and Records Administration (NARA) has assembled a forensic document examination team to study two pages of notes handwritten by H.R. Haldeman, chief of staff to President Richard Nixon, who served from 1969 to 1973.

The notes, part of NARA's permanent records collection, were allegedly written during Haldeman's 11:30 a.m., June 20, 1972, meeting with Nixon in the Executive Office Building, three days after the infamous break-in at the Democratic National Committee headquarters at the Watergate complex. During this meeting, more than 18 minutes of a tape-recorded conversation between the two men were erased before the tape was turned over to a special prosecutor in response to a subpoena.

In assembling the examination team, NARA said it hopes to clear up some mysteries surrounding the June 20 meeting. According to *The New York Times*, the forensic team will also try to determine whether any additional notes were taken by Haldeman or anyone else at the meeting, and whether the two pages were edited to remove or add notes afterward, presumably in an effort to protect the president. The ink and paper will be tested by Hyperspectral Imaging at the Library of Congress to detect light variations and indentations caused by writing on other pages. The tests can also reveal whether carbon copies were made.

Team members include experts from the Library of Congress Preservation Research and Testing Division, Treasury Inspector General for Tax Administration Forensic Science Laboratory, and Bureau of Alcohol, Tobacco, Firearms and Explosives Forensic Science Laboratory.



**Haldeman**



**OPEN RECORDS**

**U.S. Agencies Pay Millions for Public Docs**

A Freedom of Information Act request has revealed that the Department of Justice (DOJ) paid \$4.2 million in 2009 to the federal court system for access to its electronic court filing system, which contains public documents.

Open government advocate Carl Malamud, who requested the information, said an open source repository of U.S. legal records – a project he is spearheading called *Law.gov* – could ultimately save the government \$1 billion.

Public Access to Court Electronic Records (PACER) is the Administrative Office of the U.S. Courts' search system that charges citizens, journalists, lawyers, and even government officials 8 cents a page to view court filings in U.S. District Courts.

The DOJ is not alone in using the system. The IRS spent \$950,000 in 2008 to see public court documents, according to

*Wired.com*.

PACER users cited many things they disliked about the system, such as that the search function is detailed and inflexible, according to *Wired*, and the system cannot notify a user when a case is updated. Also, despite the fact PACER comprises documents in the public record, the U.S. Court system has refused to make them available for bulk download.

In addition, PACER does not include tax or Supreme Court records. To obtain those docu-

ments, DOJ paid West Publishing \$5 million in 2005 alone, according to *Wired*.

The Administrative Office of the U.S. Courts has defended the PACER system, saying citizens who sign up for accounts each get \$10 worth of free documents a year. U.S. Court spokesman Dick Carelli told *Wired* that 20% of searches on the site are free. However, he also said the court system is currently surveying users of its electronic systems and may make



**GOVERNMENT RECORDS**

**NASCIO's Top 10 Priorities for State CIOs**

The National Association of State Chief Information Officers has released the top-10 expectations it has of state chief information officers:

- 1 Budget and cost control:** managing budget reduction, implementing strategies for savings, reducing or avoiding costs, and establishing activity-based costing
- 2 Consolidation:** centralizing and consolidating services, operations, resources, infrastructure, and data centers
- 3 Shared services:** developing business models, sharing resources, services, infrastructure, which are independent of organizational structure
- 4 Broadband and connectivity:** strengthening statewide connectivity of broadband and wireless
- 5 American Recovery and Reinvestment Act:** execution, support, reporting, data management
- 6 Security:** risk assessment, security safeguards, enterprise policies, employee education, data protection, insider threat
- 7 Transparency:** open government, performance measures and data, accountability, access to government data
- 8 Infrastructure:** data centers, infrastructure investment, critical infrastructure protection
- 9 Health information:** architecture, assessment, partnering, implementation, health information exchange, technology solutions
- 10 Governance:** improving IT governance, data governance



**GOING GREEN**

## Trees Benefiting From Recession

The recession and resulting layoffs of millions of employees in the United States has reduced paper usage, an IDC analyst told *The Kansas City Star*.

Specifically, about a year ago IDC analyst Jake Wang noticed the first-ever drop in the number of pages Americans were printing. For several years from an office in Los Angeles, he has used computer software to monitor 700,000 printers and multifunctional devices in businesses.

Wang said the fourth quarter of 2008 showed a definite decline in page outputs. For the year, page output totaled 1.5 trillion – 5,000 printout sheets for every man, woman, and child. But that number fell by more than 10% in 2009, he estimated.

However, Wang expects the demand for paper will climb again when the economy does, perhaps as soon as 2011.

**ARCHIVES**

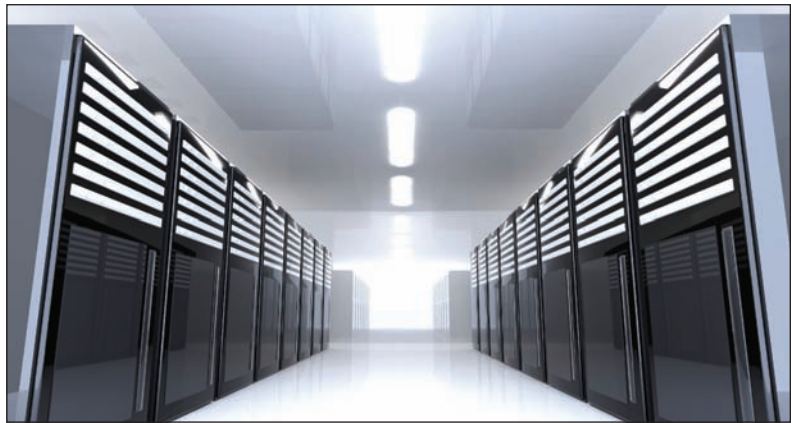
## UK Libraries Seek Power to Archive Websites

United Kingdom (UK) ministers say the UK will host 15 million websites by 2016, but under existing copyright laws, the British Library would be able to archive only about 1% of them.

To remedy this, the UK government is trying to fast-track new legal powers to allow the library to

they have lost millions of pages recording events, including the Military of Parliaments' expenses scandal, release of the Lockerbie bomber, and Iraq war, and may lose millions more because they are not legally able to "harvest" these sites, *InfoWorld* said.

The powers the libraries need are similar to copyright laws, which require every publisher in the UK to provide the libraries with copies of every printed book, magazine, journal, and newspaper. A consultation due this month would allow the libraries to copy and archive free sites with the



archive millions of websites, according to *InfoWorld*.

After almost seven years of delays, Culture Minister Margaret Hodge is pushing for these powers to be enacted quickly so six major libraries can legally copy every free UK-based website in order to record pieces of Britain's cultural, scientific, and political history, *The Guardian* reported.

UK libraries have said that

uk domain name, as well as all other UK-based sites. Subscription sites would still be closed to the copyright libraries, *Info-World* reported.

Libraries have their work cut out for them. The British Library's chief executive told *The Guardian* that by 2020, more material will be published in digital format than print, and the library must preserve and provide access to all of it.

**INFO ACCESS**

## Googling Legal Opinions

Internet users everywhere can now access full-text legal opinions online. Google Scholar (<http://scholar.google.com>) allows users to search for cases from U.S. federal and state district, appellate, and supreme courts.



**DATA SECURITY****ITRC Reports 2009 Data Breaches**

The Identity Theft Resource Center (ITRC) Breach Report recorded 498 data breaches in 2009, down from the 657 reported in 2008. But while the number of breaches may be falling, more and more records are comprised in those breaches each year – more than 222 million in 2009 alone.

breaches compromised around 80 million records in 2009.

- The financial and medical industries, perhaps because of tighter regulations, recorded the lowest percentage of breaches.
- Of all records lost last year, 46% can be traced to contractors.

	Electronic	Paper
<b>Number of breaches</b>	<b>369</b>	<b>129</b>
<b>Percentage of breaches</b>	<b>74%</b>	<b>26%</b>
<b>Number of records</b>	<b>222,286,837</b>	<b>190,206</b>
<b>Percentage of records</b>	<b>99.9%</b>	<b>0.1%</b>
<b>Total breaches in 2009:</b>	<b>498</b>	
<b>Records exposed:</b>	<b>222,477,043</b>	

Source: ITRC

Highlights of the ITRC's report include the following:

- Paper breaches accounted for nearly 26% of known breaches (an increase of 46% from 2008).
- The business sector jumped from 21% to 41% of reported breaches from 2006 to 2009, marking the fifth year in a row breaches in this sector have increased.
- Malicious attacks surpassed human error as a cause of breaches for the first time in three years.
- Of 498 breaches, only six of the affected entities reported they had either encryption or other strong security features in place protecting the exposed data.
- U.S. government and military organizations experienced 82 breaches in 2009, compared to 110 in 2008. However, fewer than three million records were hacked in 2008, while

According to the ITRC Breach Report, more than 222 million potentially compromised records in 2009 were recorded. Of those, 200 million stem from two very large breaches, including credit card processing firm Heartland Payment Systems and the National Archives, which lost a drive containing data on 76 million service members.

However, the ITRC said that in more than 52% of publicly reported breaches, no statement was provided of the number of exposed records. The ITRC indicated it is unsure just how many total records may have been exposed due to breaches last year; but it does confirm that more than 222 million records compromised in 2009 is a giant increase from the 35 million compromised in 2008.

The ITRC adds that its data breach statistics, which are collected from breach reports by reputable media and government

sources, are far from complete because there is not one comprehensive data breach list requiring mandatory public reporting. Numerous data breaches go unreported each year, and some states require breaches to be reported, but do not allow public access to those reports.

**OPEN RECORDS****West Virginia Officials Can Keep E-Mail Secret**

At a time when many state governments and public officials are opting for increased transparency, West Virginia's Supreme Court has decided the state's officials and employees can keep their personal e-mails private.

The court recently ruled 4 to 1 that none of the 13 e-mail messages between former Chief Justice Elliott E. Maynard of the Supreme Court and the chief executive of Massey Energy, Don L. Blankenship, are public records, the Associated Press (AP) reported.

The AP sued to gain access to the e-mails in 2008, when Massey had cases pending before the court. Judge Duke Bloom of Kanawha County Circuit Court ruled that five of the e-mail messages were public records because they discussed Maynard's unsuccessful campaign in the Democratic primary, in which he ran against two justices now serving on the court. After Bloom's ruling, the five e-mails were released. However, the state supreme court ruled that Bloom was wrong and sent the case back to his court.



## GOVERNMENT RECORDS

## Obama Takes on Overclassification



As part of a sweeping overhaul of the executive branch's system for protecting classified national security information, President Barack Obama has signed a new executive order (EO). The new order replaces EO 12958 that was issued by President Bill Clinton in 1995 and later amended by President George W. Bush in 2003. After a review of EO 12958, Obama's national security advisor recommended revisions to improve transparency, openness, and interagency collaboration in how the government handles national security information.

Specifically, the new order:

- Establishes a National Declassification Center (NDC) at the National Archives to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training on the declassification of records with permanent historical value.
- Establishes a policy, for the first time, under which no records may remain classified indefinitely. Also creates tougher standards that agencies must meet to exempt

records from automatic declassification after 25 years. The order prohibits records from being classified more than 75 years, except in certain circumstances. It also directs that information not be classified (or be classified at a lower level) when "significant doubt" exists about the need for classification.

- Facilitates greater sharing of classified information among appropriate parties and governments. It calls for the greatest possible access to classified information by authorized persons. The order also significantly modifies the "third agency rule" to permit re-dissemination of classified documents by receiving agencies without the approval of the originating agency, except when the originating agency has indicated on the documents that such prior approval is required.
- Tightens restrictions on reclassification of information after its declassification and release under proper authority.
- Mandates the use of stan-

dardized electronic formats and processes for the appropriate classification and declassification of electronic data.

- Requires agencies, for the first time, to conduct fundamental classification guidance reviews to ensure classification guides are up-to-date.
- Eliminates a rule put in place in 2003 by George W. Bush that allowed the intelligence community to veto certain decisions to declassify information. Instead, agencies that object to a declassification decision must appeal to the president.

According to a memo from Obama to agency heads, public access to a backlog of 400 million pages of records must be granted by December 31, 2013, *Federal Computer Week* reported.

Initially, the NDC will be located at the National Archives facility in College Park, Md. The facility will focus on clearing the backlog of referrals in reviewed documents in federal records and in presidential materials. Michael Kurtz, Ph.D., assistant archivist for the Office of Records Services, will serve as interim acting director of the NDC.

An inter-agency program management team is examining current declassification review processes throughout the government. The National Archives is working with the Defense Change Management Organization to conduct a study to determine how to improve processes by reducing process cycle time, defects, and costs. Any recommendations will be incorporated into the new NDC processes.

According to *The New York Times*, even more changes may be on the way. Gen. James L. Jones, the national security adviser, is leading a study "to design a more fundamental transformation of the security classification system." **END**