TECHNOLOGY

QR Codes: An Extra Dimension

Quick response (QR) codes, which can be scanned by smart phone users that have a QR scanning application, are showing up everywhere, including on print advertisements, product displays, and web pages. Most often, the code takes users to specific websites where they can find additional information or coupons. However, because the two-dimensional barcode can hold thousands of alphanumeric characters of information, its use is expanding in ways that could have information management implications.

For example, the manufacturer of MedFlash, a system for maintaining electronic personal health records, announced in August that it would begin adding QR codes to its users' emergency identification cards so first responders can scan them to retrieve emergency medical information. It is a great benefit, Connectyx said, because most first responders have a smart phone with them at all times, and QR scanning applications for these phones are available to download free from Apple, AT&T, BlackBerry, and many others.

Because QR codes can store so much more information than a standard barcode, they are also being considered for use by at least one commercial records storage and management company for indexing and managing records.

It is easy and inexpensive for any organization to incorporate QR codes into internal or external communications. Some of the better-known QR code-generating sites are Kaywa, Qurify, and Delivr.

Attendees at ARMA International's 56th Annual Conference & Expo, October 17-19, in Washington, D.C., should be ready with their smart phones and QR scanning application, as some exhibitors are sure to be making use of this technology to provide additional value on the show floor.

Scan this code to access *Information Management* online!

GOING GREEN

Airlines Testing Paperless Cockpit

Pilots routinely drag flight bags weighing 35 pounds or more full of paper flight materials with them to the cockpit, according to National Public Radio (NPR).

But a few airlines have found that by making such data digital, they can save more than $1.2 million annually in fuel costs. American Airlines and the Allied Pilots Association (APA), the union for the airlines' pilots, are testing the use of iPads "from gate to gate during all phases of flight," according to an American Airlines spokesperson.

The Federal Aviation Administration (FAA)-approved tests, which began in June with Los Angeles-based pilots using iPads on two flights headed to Shanghai, will last for six months, American said. The tests are a final step before the FAA approves iPads for use as electronic flight bags, allowing crews to perform many tasks that today are mostly handled by paper. The iPads include reference materials, including navigational charts and flight manuals, as well as electronic charting capability, which offers pilots a digital image of their route, *The Washington Post* reported.

"By eliminating bulky flight bags filled with paper, [electronic flight bags] mean less weight for pilots to carry, reducing the possibility of injury on duty," First Officer Hank Putek, a member of the APA safety committee, said in a statement. "In addition, they enable pilots to immediately download updates, rather than waiting for paper versions of required documents to be printed and distributed."

In May, Alaska Airlines began transitioning to paperless flight plans, according to *Apple Insider*.

The FAA previously classified iPads as a "class 1" electronic device, meaning it must be stowed during takeoff and landing, even by pilots. However, *Apple Insider* said the FAA has since specifically approved the use of the iPad app providing tables and other info for use during all phases of flight, marking the first time a tablet PC has been usable during takeoff and landing.

WEB

U.S. Government Reduces Web Presence

Over the next year, the Obama administration plans to shutter or consolidate about half of the government's 2,000 top-level websites to save money, the White House said.

Over the summer, the administration had ordered a 90-day freeze on all new ".gov" websites unless agencies could prove a "compelling need." *The Washington Post* said budget cuts have also forced the White House to cancel two new websites related to President Barack Obama's open government efforts. The Office of Management and Budget is shuttering a site that would have allowed federal employees to exchange work tips and information. Another, also cancelled, would have provided information on the quality of federal services to the general public.

According to *The Post*, the administration had little choice after budget cuts reduced the Electronic Government Fund from $35 million to $8 million. The fund helps finance the government sites that track federal data (*Data.gov*), government contracting (*USASpending.gov*), government information technology (*IT Dashboard*), and overall federal employee performance (*Performance.gov*).

By October, *The Federal Times* reported, agencies will identify websites that can be eliminated or consolidated and will then report the actions they take to complete the job.

The Energy Department's director of new media said ending the creation of new websites and closing others have saved that department more than $1 million over a six-month period. Cammie Croft, deputy new media director at the White House, blogged that the department estimates saving $10 million annually by consolidating hardware, hosting services content, and IT systems.

Skeptics have questioned the initiative's real savings. IT experts say what may cost the government, according to open government advocates, is the possibility of losing valuable data as websites are shuttered. But according to *The Federal Times,* the government doesn't track how much agencies spend to create and maintain the more than 24,000 .gov websites. Hardware, software, and content expenses are usually included in larger IT budgets, making it hard to determine actual costs.

Before he resigned, former Federal Chief Information Officer (CIO) Vivek Kundra said the *IT Dashboard* has helped save the government $3 billion on IT projects. "Using this important tool, we identified underperforming high priority IT projects and began an intensive review of these programs, eliminating ineffective projects, reconfiguring others, and targeting IT expenditures more carefully," he said in a video blog.

The move to slash websites seems to undercut Obama's push for more government transparency.

"The open government initiative is pushing us to make things more readily available to people," John Hopkins, chief of staff for NASA's CIO, said. "We don't want to be closing down things that are actually facilitating open government."

Daniel Schuman, policy counsel for the Sunlight Foundation, said there is no precedent for decreasing the government's web presence. "If the administration is going to reduce the number of websites, will they find a home for the information housed by these sites?"

PRIVACY

Texas Enacts New Health Privacy Law

After an embarrassing data breach that exposed the personal information of more than 3.5 million Texans on a public government server for more than one year, Gov. Rick Perry has signed into law an expansive new health privacy bill.

The law's requirements exceed those of the federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, legal experts say. The law, which becomes effective Sept. 1, 2012, includes a broad definition of the term "covered entity" in Texas' existing health privacy law and may affect many non-HIPAA-covered entities.

Under the Texas law, "covered entity" includes any organization that engages in "assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information," as well as any entity that "comes into possession of" or "obtains or stores" protected health information (PHI).

The new law also:

- Requires employees of covered entities to undergo training on HIPAA and Texas' health privacy law within 60 days of hiring (and at least once every two years)
- Bans the disclosure of PHI for remuneration, but covered entities may disclose PHI to other covered entities for treatment, payment, healthcare operations, insurance, or HMO functions, or as authorized or required by federal or state law
- Requires covered entities to notify individuals that their PHI is subject to electronic disclosure and obtain consent for any electronic disclosure of PHI (except disclosures of PHI to other covered entities)
- Requires healthcare providers to give access to an individual's PHI within 15 days of the request
- Authorizes the Texas Attorney General, Texas Health Services Authority, or Texas Department of Insurance to conduct compliance audits of covered entities that have consistently violated the Texas law
- Requires the Texas Health Services Authority to develop privacy and security standards for the electronic sharing of PHI

E-MAIL

Court: E-Mails Not Covered by FACTA

The Ninth U.S. Circuit Court of Appeals recently concluded that an e-mail is not an "electronically printed" receipt under the Fair and Accurate Credit Transactions Act (FACTA).

FACTA, which went into effect in 2006 and is meant to help fight identity theft, bars businesses that accept credit cards from printing more than five digits of a card number or expiration date on a receipt. The law, as written, applies to electronically printed receipts, but doesn't define that term, according to *The American Lawyer*.

The Ninth Circuit's ruling stems from a 2009 case involving Dimitriy Simoff and Expedia. Simoff claimed the travel website violated FACTA by including Simoff's card's expiration date in an e-mailed receipt.

In June 2010, a Seattle federal district judge ruled that the phrase "electronically printed" referred only to actual receipts printed by cash registers and dismissed the case against Expedia. Two months later, in a similar case, a different court ruled that 1-800 Contacts' e-mailed receipts did not violate the law, *The American Lawyer* reported.

The Ninth Circuit Court upheld the dismissal, finding for Expedia that FACTA's language "simply leaves no room to doubt" that e-mailed receipts are not covered by the law. Further, the court concluded the law specified electronically printed receipts only to distinguish receipts that are printed by a machine because FACTA exempts the type that is created with an impression of the card.

This case is just one of many recent cases that have been concerned with the same issue. Legal experts say the Ninth Circuit's Simoff decision may cement the growing consensus that FACTA should be applied as written and should not be used to create prohibitions that Congress did not explicitly authorize.

CONSUMER RECORDS

FTC Approves Facebook Archivings

Facebook files are fair game when it comes to investigating employees and potential employees, the U.S. Federal Trade Commission (FTC) said.

The FTC has approved the Social Intelligence Corp.'s practice of archiving Facebook users' posts as part of a background-checking service. The commission said the company complies with the Fair Credit Reporting Act (FCRA), which also allows the retention of consumer credit records for seven years.

If something negative about an individual pops up on Facebook or Craigslist when a search is made, Social Intelligence puts it into the individual's file and retains it for seven years, according to a *Forbes* report. But records that are disputed and changed are deleted and replaced by new material. Also, new employers who run searches through Social Intelligence won't have access to the materials if they are completely removed from the Internet.

Social Intelligence's Chief Operating Officer Geoffrey Andrews explained to *Forbes* that while negative information is kept on file, it is not reused when a new employer runs a check on a person.

"While we store information for up to seven years, we do not 'reuse' that information for new reports. Per our policies and obligations under the FCRA, we run new reports on applicants on each new search to ensure the most accurate and up-to-date information is utilized, and we store the information to maintain a verifiable chain-of-custody in case the information is ever needed for legal reasons. We are not however building a 'database' on individuals that will be evaluated each time they apply for a job and potentially could be used adversely even if they have cleaned up their profiles."

Andrews said some of the reports his company has provided to employers so far have included a job applicant who posted a photo on a social networking site that featured multiple guns and a sword, and another who was assumed to be a racist for joining a Facebook group called, "I shouldn't have to press 1 for English. We are in the United States. Learn the language."

Social Intelligence mines public data from social networking websites (e.g., Facebook), professional networking websites (e.g., LinkedIn), blogs, wikis, video, and picture-sharing websites, Andrews said.

For the practice to comply with FCRA, a job applicant must acknowledge and approve the use of a social media background screen, just as they would a criminal and credit background check. Still, individuals should be cautious about posting questionable content online, just in case it's captured and filed away for future employers.

PRIVACY

U.S.-EU Air Passenger Data Deal Illegal, Lawyers Say

The United States and European Union (EU) have hammered out an agreement on storing the personal data, including credit card details, home addresses, and phone numbers, of millions of transatlantic travelers, but the European Commission's lawyers have warned that the deal's 15-year storage requirement is illegal.

According to *The Guardian*, the legal opinion states that the agreement to allow the U.S. Department of Homeland Security (DHS) to store airline check-in data is "not compatible with fundamental rights" or EU data protection law.

The agreement would allow passenger data provided to airlines at check-in to be analyzed by U.S. data mining and profiling programs to help fight crime, terrorism, and illegal immigration. The United States wants airlines to supply the passenger lists 96 hours before takeoff so it can check them against various watch lists, *The Guardian* reported.

With the 15-year retention requirement, the U.S.-EU passenger name record's (PNR) retention period is three times the five years allowed for in the EU's PNR. A period of five and a half years was recently negotiated in a similar agreement with Australia, *The Guardian* noted.

The agreement must get approval from the Parliament and ministers before it can become law. The European Parliament has demanded proof that such a PNR agreement is necessary, and said it should in no circumstances be used for data mining or profiling. U.S. lawmakers have said the agreement is an important tool for security agencies to help them identify possible threats before they arrive in the country.

According to *The Guardian*, the U.S.-EU agreement tries to allay some privacy concerns by proposing to "mask" or "depersonalize" the identity of individuals after six months on the DHS's active database. The data will be transferred to a dormant database after five years, to be held for 10 more years. But the agreement allows for individuals' identities to be restored at any stage by authorized officials if needed for a law enforcement operation.

The Guardian reported that while Britain, Estonia, Ireland, and Sweden support the PNR agreement and database, France, Germany, Italy, and Netherlands remain strongly critical.

The European lawyers said they also are concerned because the agreement states that oversight will be carried out by U.S. DHS officials rather than independent officials. They also pointed out the agreement does not provide proper access to the courts for those individuals seeking redress for misuse of their data. All forms of redress are administrative only and are subject to U.S. law, according to the deal.

OPEN RECORDS

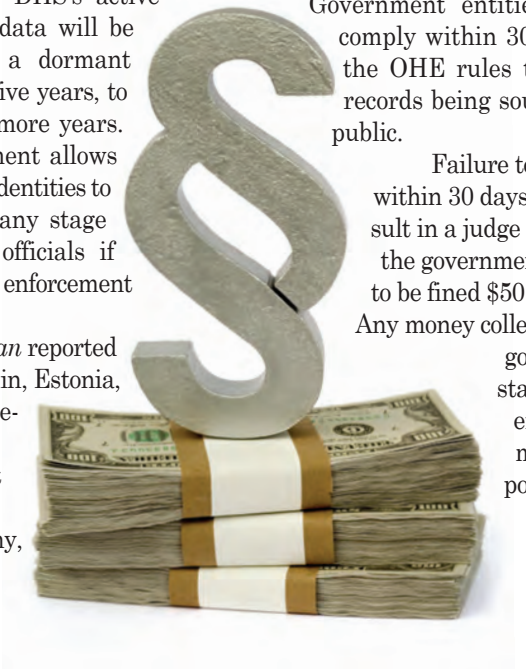
S.D. to Fine Open Records Violators

State and local agencies that drag their feet in responding to open records requests in South Dakota will now face hefty fines for their inaction.

A law that took effect July 1 allows a $50 a day fine for government entities that delay records requests. The law was added to the state's 2009 open records law.

Individuals who seek government records and are denied access can appeal through the state Office of Hearing Examiners (OHE). Government entities must comply within 30 days if the OHE rules that the records being sought are public.

Failure to comply within 30 days may result in a judge ordering the government entity to be fined $50 per day. Any money collected will go into the state's general fund, media reports said.



COURT RECORDS

Kansas City Court Goes Digital

It's being called the biggest digital transformation of a municipal court in the United States, and other cities are watching closely.

"It is the first municipal court to go end-to-end paperless," said Austin, Texas-based technology consultant and project manager, Alan Teeple, in an interview with *The Kansas City Star*. He said courts in other cities, including St. Louis and Memphis, Tenn., are keeping an eye on Kansas City, Mo.

Kansas City's new paperless court system was set to go live August 29, according to *The Star*, and it is a radical departure from the municipal court's 40-year-old law enforcement and records system it is replacing.

The old system relied on an ancient IBM mainframe, an extinct computer language, and a mountain of paper records, *The Star* said. Presiding Municipal Judge Katherine Emke said the court was drowning in a sea of 1.5 million active paper files. Each year brought a deluge of 320,000 tickets and 30,000 phone calls every month.

According to *The Star*, paper records were strewn throughout the building, and data entry clerks made mistakes. It often took an hour or more to pull just one person's file. Tickets, which were kept in giant rotational filing machines, would get stuck together or lost. If the machines broke, *The Star* said, only one 79-year-old maintenance person in the city knew how to repair them.

The new, digital system includes three components, says *The Star:* e-ticketing for all traffic and municipal violations; a regional database to share offenders' criminal histories throughout the metro area; and a new court case management system.

The project has a price tag of nearly $6 million, including consulting fees, new software, and 600 handheld computers and miniprinters, and was derived from court fees, a public safety sales tax, and other technology funds.

In return, city officials say they expect the system to save the court $1 million annually in reduced staffing, paper, and other operation costs. Other improvements include:

- Easier, faster access to court records for lawyers, who say it will help them represent their clients better
- Improvements in court scheduling and efficiency, reducing crowding and waiting
- An interactive website that allows people to pay fines, check court dates, or request a continuance online

HEALTH RECORDS

HHS Issues New HIPAA Rule

The Department of Health and Human Services (HHS) recently issued a proposed rule that modifies the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule's standard for the accounting of disclosures of protected health information (PHI).

This proposed rule addresses changes mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, which requires HIPAA-covered entities and business associates to account for PHI disclosures made through an electronic health record for the purpose of treatment, payment, and healthcare operations.

The proposed rule divides the accounting rights into two distinct individual rights. The first follows the long-standing accounting of disclosure rules, modifying the existing rule to require an accounting for three years before an individual's request instead of the current six years. The second offers individuals a new right to receive a written "access report" that describes uses and disclosures of their PHI made through an "electronic designated record set."

This report would include information on a covered entity's workforce members who have accessed information and would apply to information in an electronic designated record set, not only information in an electronic health record, as required by HITECH.

The proposed rule was published in the *Federal Register* May 31 and is available at *www.ofrgovOFRUploadOFRData/2011-13297_PI.*

CONSUMER RECORDS

Supreme Court Approves Data Mining by Drug Cos.

The U.S. Supreme Court has struck down a Vermont law that restricted data mining and drug companies from using prescription information for marketing purposes.

Pharmacies are required by state and federal law to collect the information, which typically includes doctors' names, what drugs they prescribe, and how often drugs are ordered. Pharmacists sell the data to data mining companies, who then sell it to drug makers with patient names removed or encrypted, *InformationWeek* said.

The 2007 Vermont law effectively banned the practice in the state. It said data mining companies can't sell the prescription information for marketing purposes, and drug makers can't use it unless the prescribing doctor consents. Vermont lawmakers said the measure would protect the privacy of doctors and patients and help to control the cost of expensive brand-name drugs.

According to the Associated Press (AP), brand-name drug makers spend an estimated $8 billion annually marketing their products to doctors.

Those efforts include the practice of detailing, in which sales representatives target individual doctors based on the doctors' own prescribing habits, the AP reported. The law banned detailing, but still allowed the information to be used for healthcare research and educational purposes, and by law enforcement, insurance companies, and journalists.

The lawsuit said the information about doctors' prescribing patterns is important in helping spot trends, tracking the safety of new medications, and studying treatment outcomes. The data mining companies make such data available to researchers and the government at little or no cost.

In the case *Sorrel v. IMS Health, Vermont* argued: "By letting doctors, rather than the state control the use of this information for marketing, the legislature avoided impinging on the 'protected interest' in communication between pharmaceutical manufacturers and willing doctors."

IMS Health, SDI Health, and Source Healthcare Analytics said their actions are protected by the First Amendment. They stated pharmacists have a constitutional right to share prescription data and drug companies have the right to use it.

Lower courts have disagreed on whether laws like Vermont's were constitutional. According to AP reports, a federal appeals court in New York ruled against the Vermont law, but a different appeals court upheld similar laws in Maine and New Hampshire, saying they regulated only the conduct, not the speech of data miners.

The Supreme Court, however, declared the Vermont law unconstitutional on grounds that it violates the drug industry's free speech right to market its products. In a 6-3 decision, the court ruled that states can't stop drug makers and data mining companies from using information about the prescription drugs individual doctors prescribe.

The ruling imperils similar laws in Maine and New Hampshire, the AP reported.

CYBERCRIME

Canada: A Growing Haven for Web Crime

A recent Websense survey conducted by an online security firm ranked Canada as the second most popular host for phishing sites, which attempt to acquire sensitive information (e.g., usernames and passwords). The United States ranked first.

According to the survey, phishing sites have grown by 319% in Canada over the past year, and bot networks have increased by 53%. The survey also revealed Canada is a growing center for bot networks used by hackers to perform malicious tasks or functions.

According to an *SC Magazine* article, Canada Privacy Commissioner Jennifer Stoddart has voiced her concerns about the "alarming trend toward ever-bigger data breaches" and called for "significant attention-getting fines" for companies whose poor security practices allow users' information to be compromised.

Stoddart also announced her intention to recommend that Industry Canada amend previously introduced legislation to include hefty fines when it is resubmitted for debate in Parliament.

E-DISCOVERY

Scheindlin Retracts Metadata Ruling

Federal Judge Shira Scheindlin has retracted a recent 27-page opinion that extended the boundaries of metadata produced by government agencies in response to Freedom of Information Act (FOIA) requests.

Scheindlin's previously filed court opinion involved the case *Nat'l Day Laborer Org. Network v. United States Immigration and Customs Enforcement Agency* and stated that the metadata maintained by an organization as part of an electronic record is assumed to be producible under FOIA unless the organization can prove the data is not "readily reproducible." Her February opinion also specified guidelines on the minimum amount of metadata that should accompany any "significant collection of ESI [electronically stored information]."

Scheindlin said "subsequent submissions" caused her to conclude that her prior decision "was not based on a full and developed record." The 100-word reversal, entered June 17, invalidated the February ruling and as a result has muddied the state of several important e-discovery issues, according to the Association of Certified E-Discovery Specialists.

Scheindlin's withdrawal was seen as a victory for the government because the ruling had affixed a heavy obligation of providing metadata in public requests to FOIA. She noted in her June reversal ruling that the federal agencies, the National Day Laborer Organizing Network, and other immigration groups that had sued for alleged noncompliance with the FOIA request had "recently resolved their dispute regarding the form and format in which records will be produced." Her reversal came just one day after the parties announced the agreement and after a motion by the government to stay implementation of Scheindlin's February orders.

The government has maintained that "certain metadata" is not "readily producible" for FOIA purposes. Without a hearing and a factual record, government lawyers argued, Scheindlin had no basis by which to require that the government produce metadata. They also questioned whether metadata can be considered a record or an "integral or intrinsic part" of a record in responding to FOIA requests. In her ruling, Scheindlin said, it is "well accepted, if not indisputable that metadata is generally considered to be an integral part of an electronic record."

By withdrawing her decision, Scheindlin noted, the prior ruling should "have no precedential value in this lawsuit or in any other lawsuit." Scheindlin wrote that "regardless of whether FOIA requests are subject to the same rules governing discovery requests, [*Federal Rules of Civil Procedure*] Rule 34 surely should inform highly experienced litigators as to what is expected of them when making a document production in the twenty-first century." Rule 34 specifies the obligations of federal litigants in "producing documents, electronically stored information, and tangible things …"

But, according to several legal experts, an FOIA lawsuit is not an ideal setting in which to establish metadata standards. They say Scheindlin was trying to establish that all discovery requests in legal settings follow the same rules, but comparing business to government is like comparing apples and oranges.

DATA SECURITY

Russia Amends Federal Data Protection Law

The upper house of Russia's federal legislature has approved amendments to the country's federal data protection law that mandate strict information security requirements for businesses that process personal data. The amendments also revise some of the statute's data consent provisions.

Russia's comprehensive federal data protection law was passed in 2006, but heavy criticism delayed its actual implementation until July 1, 2011. Observers say the law is similar in approach to the EU's Data Protection Directive, but places far more restrictions on the processing of personal data.

According to the Information LawGroup, the amended security provisions require businesses to:

- Conduct a threat assessment of the safety of personal data and the effectiveness of the measures that the business has in place to safeguard personal data
- Use only verified methods of protecting personal data
- Implement controls for access to personal data
- Log all actions with respect to personal data
- Detect and record incidents of unauthorized access to personal data
- Implement measures to restore information that is lost, destroyed, or damaged as a result of a data breach

The amended law directs the government to develop regulations that will establish appropriate levels of data security protections and establish the security requirements for processing biometric data.

The federal law's privacy provisions were amended to allow individuals to approve the processing of their personal data through a representative. When this occurs, the recipient of the consent must verify it. Similarly, businesses may obtain personal data from third parties if they verify that the third party had a valid basis for obtaining and sharing the information.

E-RECORDS

European-Sponsored DLM Forum Releases MoReq2010

The DLM Forum, a European Commission-sponsored community interested in archive, records, document, and information lifecycle management throughout Europe, recently announced the publication of the core services and plug-in modules for the Modular Requirements for Record Systems (MoReq2010) specification for electronic records management systems (ERMS).

This comes after two public consultations that garnered more than 500 comments and contributions from individuals, suppliers, industry associations, and the European Commission Experts' Review Group, according to the DLM Forum.

MoReq2010 is a modular approach that helps governments and businesses value, create, use, store, reuse, and destroy information appropriately to ensure that lack of information governance does not result in corporate liability. The DLM Forum said it expects most European countries will adopt MoReq2010 as a harmonized approach to information management, with the support of all the leading vendors.

"The MoReq2010 project team has reviewed and taken account of the considerable amount of input received from academic, government and commercial sources," said Jon Garde, author of MoReq2010. "The modular approach has refined the requirements and its underlying information model. An innovative service-based architecture provides the platform for the core requirements, which include interoperability and federation capabilities. These enable organizations to connect archives together, to 'future-proof' their investment as technology develops. Therefore MoReq2010 can form the basis of successful purchasing and implementations."

Developers said they focused on embracing and extending key international standards. By the end of 2011, they said, users and vendors will see the new extension modules, training programs in the United States and Europe, and the beginning of the first testing systems for the core services.

The MoReq2010 code services specification can be downloaded from *www.moreq2010.eu*.

LEGISLATION

Ohio Makes it Harder to Profit from Records Destruction

The Ohio legislature and state supreme court have decided that people should not profit from records-destruction cases.

Lawmakers recently passed a measure to cap the civil penalties for improperly destroying public records to $10,000 per case. Before it was signed into law by Gov. John Kasich, there was no limit on fines an agency could be ordered to pay when sued for destroying records – damages of $1,000 per destroyed record were possible, according to *The Columbus Dispatch*. The new law also limits attorney fees to $10,000 and requires suits to be brought within five years of the destruction.

Supporters of the new law said it will stop people from requesting records they don't want, but knew were destroyed, so they could sue and cash in.

But critics of the new law worry that it may encourage local governments to destroy potentially incriminating or embarrassing information because the maximum civil fine is only $10,000.

State Sen. Bill Seitz (R), a Cincinnati lawyer, said if government officials destroy records to cover up corruption, they still could face criminal charges, such as obstruction of justice and tampering with records.

"If anybody thinks that a $10,000 penalty and $10,000 in attorney fees is not a sufficient deterrent, then I would remind them that if the destruction is willful ... we have a whole battery of criminal laws that still apply," he said.

The law was prompted by a $1.4 million court ruling against the city of Bucyrus for recording over more than 911 tapes from the 1990s. (The Bucyrus case is back in county court after being overturned on appeal.)

Meanwhile, the Ohio Supreme Court recently decided to forbid the collection of damages for the illegal destruction of records when it is apparent that money, rather than access, is the plaintiff's main motivation.

In the case *Rhodes v. New Philadelphia*, Timothy Rhodes filed a lawsuit seeking almost $5 million in damages from the illegal destruction of old reel-to-reel tape recordings of police dispatch calls between 1975 and 1995, according to *The Dispatch*.

A jury determined Rhodes should not receive any damages and was not "aggrieved" because he did not seek access to the records; he just wanted money. He also had tried to attain old police and 911 tapes from eight other communities.

An appeals court reversed the jury's finding, ruling that Ohio law makes parties automatically aggrieved and entitled to damages of $1,000 for each destroyed record, or $84,000 in Rhodes' case. The case was then sent to the Supreme Court, which agreed with the jury.

According to *The Dispatch*, the ruling could kill similar records-destruction cases around the state if defense lawyers can prove those individuals seeking damages are primarily motivated by the collection of damages.

FOIA

FOIA Celebrates 45 Years; Backlogs Persist

Open government advocates may celebrate the fact that 2011 marks the Freedom of Information Act's (FOIA) 45th birthday, but they likely are not proud of the fact the single oldest records request is now 20 years old, according to the National Security Archive (NSA) at George Washington University.

Eight federal agencies now have FOIA requests a decade old, according to the NSA's 2011 Knight Open Government survey. FOIA requires agencies to process and respond to a request within 20 business days and allows a 10-day extension under "unusual circumstances."

The day after his January 2009 inauguration, President Barack Obama reversed the Bush-era policy of defending any legal reason to withhold information and ordered agencies to release records unless doing so was barred by law or would cause harm. But two Knight Open Government surveys conducted during the Obama administration have shown that, despite the president's order, government agencies have been slow to improve their FOIA processes.

The 2010 Knight survey, "Sunshine and Shadows," revealed that only 13 of 90 agencies had implemented concrete changes in response to Obama and Attorney General Eric Holder's early memoranda calling for FOIA reforms. The 2011 Knight survey, "Glass Half Full," showed some improvement – 49 of 90 agencies had followed specific tasks mandated by the White House to improve their FOIA performance.

For the survey, the NSA requested copies of the 10 oldest records requests from the top-35 agencies. According to the NSA, none of the requests should have required years to fulfill; most were for identifiable materials that should have been easy to locate. The NSA said several of the requests related to social-interest subjects, including whistleblowers, consumer protection, and business. But six months after the NSA requested the information, nine agencies still had not responded.

Oldest Outstanding FOIA Requests by Agency (as of December 2010):

National Archives and Records Administration	May 1991
Defense Intelligence Agency	Aug 1993
U.S. Air Force	April 1995
National Security Agency	May 1996
Central Intelligence Agency	October 1998
U.S. Army	January 2001
U.S. Department of State	February 2001
U.S. Department of Energy	February 2001
U.S. Department of Health and Human Services	October 2001
U.S. Department of the Interior	October 2002

Source: National Security Archive

The Knight survey found that 14 of the agencies analyzed have actually lost ground; their current oldest request is older than it was one year ago.

The archive determined the main reason for the increasing backlogs is the referral process. For example, any agency that claims an ownership stake in the information can seek to prevent its release, the Associated Press (AP) said. Many of the most-delayed records involve several agencies.

For instance, the single oldest FOIA request – one made to the National Archives and Records Administration 20 years ago for various state department files about nuclear research from the 1950s – is likely being held up by a referral to the U.S. Department of Energy, Nate Jones, NSA's FOIA coordinator, told the AP.

Other long-standing requests include those to presidential libraries, which typically need clearance from federal agencies. They include a 1995 request to the Reagan Presidential Library for documents about "whether American POWs and MIAs were left in Southeast Asia"; a 1998 request to the George H.W. Bush Library for documents related to the December 1988 bombing of Pan Am flight 103; and a 2000 request to the Kennedy Presidential Library for documents about "politics and the Internal Revenue Service." Also outstanding is a 2005 "urgent request" to the Transportation Department for whistleblower complaints to be used in an Occupational Safety and Health Administration hearing.

STUDY

No End in Sight to the Digital Data Deluge

The world's information is doubling every two years, according to IDC, with 1.8 zettabytes (1.8 trillion gigabytes) created and replicated this year alone. That's enough information to fill 57.5 billion 32GB iPads.

The 2011 IDC Digital Universe Study sponsored by EMC includes the vast amount of data that is created and stored, as well as transient data that is typically not stored, including digital television signals for shows watched, but not recorded.

The study highlighted the consequences of storing, managing, and securing all that information. Over the next 10 years, the study said, the number of servers (virtual and physical) around the world will increase 10-fold, the amount of data management by data centers will increase 50-fold, and the number of files they will have to process will increase at least 75-fold. Meanwhile, IDC noted, the number of IT professionals in the world who are responsible for managing all that information will only grow by a factor of 1.5.

Other findings include:

- Since 2005, annual enterprise investments in the cloud, hardware, software, services, and staff to create, manage, store, and generate revenue from information have increased 50% to $4 trillion.
- Although cloud computing accounts for less than 2% of IT spending now, almost 20% of information will be "touched" by the cloud by 2015 somewhere in a byte's journey from originator to disposal.
- Too much data remain vulnerable to hackers and thieves. IDC estimates about half the information that should be protected in the digital universe are protected.
- In 2011, the cost of creating, capturing, managing, and storing data was down to one-sixth of what it was in 2005.
- Since 2005, annual investment by enterprises in the digital universe has increased 50% to $4 trillion – that's money spent to create, manage, store, and derive revenue from the digital universe.

IDC's findings call for big changes for the data center industry. The research firm said the demand for physical storage space will continue to grow, and data centers will need to adapt to keep up with that demand. IDC predicts increased automation and a shift toward new infrastructures developed to enable cloud computing and "big data."

One of the biggest challenges involves how to manage huge datasets and extract business value from them. "Big data will inject high-velocity requirements associated with capture and analysis, as well as results/predictive reporting," IDC writes. "Big data deployments require new IT administration and application developer skill sets. People with these skills are likely to be in short supply for quite a while."

At the present rate, IDC estimates that about 7.9 zettabytes will be created in 2015. **END**

A Decade of Digital Universe Growth

- 2005 – 130 exabytes
- 2010 – 1,227 exabytes
- 2015 – 7,910 exabytes

Source: "2011 IDC Digital Universe" study

HEALTH RECORDS

Google Ends EHR Service

Google has decided to end its electronic health records (EHR) initiative after three years. According to *The New York Times*, Google Health failed to attract enough users. The service required users to enter, update, and edit their health data online. By contrast, the U.S. government's EHR initiative offers up to $40,000 in incentives for hospitals and doctors who move patients' paper records online.

Analysts say EHRs are new to most people, and even early adopters have found them difficult to use. "Personal health records have been a technology in search of a market," Lynne A. Dunbrack, an analyst at IDC Health Insights, told *The Times*.

To illustrate the challenge for Google Health, a 2011 IDC Health Insights survey found that 7% of consumers had tried online EHRs, and fewer than half of those individuals continued to use them.

But Google is not the only business to abandon the consumer health records space. *The Times* said Revolution Health retired its personal health record service last year due to too few users.

Other providers of online personal health records include WebMD, Microsoft, RelayHealth, and Dossia. But analysts note that most of these providers work in partnership with insurers and health providers, while Dossia is an employer-sponsored personal health record.