PRIVACY

EU, U.S. Agree on New Data Transfer Deal

After three months of intermittent talks, U.S. and European officials have reached a new agreement on how digital data will be transferred from one side of the Atlantic to the other. The Privacy Shield agreement, which still requires political approval, means European data protection authorities will not restrict data transfers as they had planned to if an agreement had not been reached.

According to Reuters, the European Commission said Privacy Shield will place stronger obligations on U.S. companies to protect Europeans' personal data and ensure stronger monitoring and enforcement by U.S. agencies than the previous Safe Harbor agreement.

Since Safe Harbor was invalidated by the European Court of Justice in October 2015, about 4,000 U.S. companies that had relied on it to collect and transfer data out of the EU have been without any legal guidelines for handling information ranging from financial information to social media posts.

"We have for the first time received detailed written assurances from the United States on the safeguards and limitations applicable to U.S. surveillance program," Commission Vice-President Andrus Ansip told the media. "On the commercial side, we have obtained strong oversight by the U.S. Department of Commerce and the Federal Trade Commission of companies' compliance with their obligations to protect EU personal data."

Per the agreement, the United States will create an ombudsman within the State Department to handle complaints and inquiries forwarded by EU data protection agencies, Reuters reported. There will also be an alternative dispute resolution mechanism to resolve grievances, as well as a joint annual review of the agreement.

European data protection authorities said they will also work with the U.S. Federal Trade Commission to police the system.

E-RECORDS

Still Seeking the Paperless Office

Thirty-five years ago, a British-American information scientist introduced the concept of a paperless office. Today, it seems, we are no closer to attaining that scenario, according to a recent survey of UK offices.

Printer company Epson surveyed more than 3,600 European employees, and 83% called the paperless office "unrealistic." It found that hard copies are preferred over digital documents because workers feel the need to share, hand out, and edit reports. In fact, the majority of respondents felt they'd be more likely to make a mistake when editing an electronic document than a paper copy.

According to the survey, 83% of office workers in Europe said a ban on printing would "limit their productivity." Across Europe, office workers spend nearly 19 hours every year walking to and from printers, Epson said, walking more than 110 kilometers (68.35 miles) in the process.

Another survey, from information management firm M-Files, found that 77% of UK businesses still store and manage paper records, with 19% stating they keep all records in paper format and 58% storing data in both paper and digital formats.

PRIVACY

VW Cites Privacy Laws in Refusing to Provide Documents

Volkswagen has refused to provide its executives' e-mails and other communications to U.S. attorneys general who requested the documents as part of their investigations into the company's emissions scandal, according to the *New York Times*.

In September 2015, Volkswagen admitted to installing software to cheat on emissions tests in 11 million diesel vehicles sold worldwide. The *Times* reported that a 48-state civil investigation is being led by several states, including New York and Connecticut, and attorneys general in California and Texas are also looking into the company, which includes the Audi and Porsche brands.

An inquiry by the U.S. Justice Department states that Volkswagen had "impeded and obstructed" regulators and provided "misleading information." Investigators say Volkswagen's actions limit their ability to identify which employees knew about or sanctioned the emissions cheating. Penalties would be greater if the states and others pursuing Volkswagen in court could prove that top executives were aware of or directed the activity.

German investigators said Volkswagen is working with them under the auspices of German law. Klaus Ziehe, a spokesman for prosecutors in Braunschweig, a city close to Volkswagen's headquarters in Wolfsburg, said German law allowed prosecutors to carry out raids of Volkswagen's Wolfsburg offices to gather possible evidence that could include e-mail exchanges, the *Times* reported.

"We can't complain about our cooperation with the company," Ziehe said. "We have the impression that we have received everything that we have specifically requested."

Germany is known for its strict privacy laws, which limit access to data, especially for those outside the European Union. In refusing to turn over evidence to American investigators, Volkswagen has cited the German Federal Data Protection Act, as well as the German Constitution, the European Convention on Human Rights, decisions of the German Constitutional Court and the European Court of Human Rights, "and (for good measure) provisions of the German Criminal Code," according to the *Times*.

INFO SECURITY

Survey: Departing Employees Take Sensitive Data

More than one in four employees take and/or share sensitive company data when leaving a job, according to a recent survey from secure communications solutions provider Biscom.

Technology decision-makers take heed: Survey findings show that the technology a company implements plays a major role in an employee's' decision to take company data. For example, tools like Dropbox, Google Drive, and e-mail make it effortless to take files.

The survey also found:

- 15% of respondents said they are more likely to take company data if they are fired or laid off than if they leave on their own.
- Of those who take company data, 85% report they take material they have created themselves and don't feel doing so is wrong.
- Only 25% of respondents report taking data they did not create.
- About 95% of respondents said that taking data they did not create was possible because their company either did not have policies or technology in place to prevent data stealing or it ignored its policies.

"The survey's results reveal employees as a big security hole," John Lane, CISO of Biscom, said in a statement. "Companies can use this information to understand how they can protect their data. Whether it's updating employee training, establishing stricter company policies to prevent data theft, or obtaining secure tools to store and track company data."

Although stealing data can result in significant security risks, most survey respondents reported that they didn't view it as data theft. Despite the fact that they're taking sensitive information, including company strategy documents, customer lists, and financial data, employees don't consider their actions malicious or even wrong. The report concluded that this may be why data theft is so prevalent.

CYBERSECURITY

Canadian Organization Releases Cybersecurity Guides

A self-regulatory organization that helps monitor Canada's trading industry has released two guides to help investment dealers protect themselves and their clients in the event of a cyber attack.

The Investment Industry Regulatory Organization of Canada (IIROC) introduced "Cybersecurity Best Practices Guide" as a living document that can be updated to include the latest practices on governance and risk management, network security, and more. The 53-page guide also features a cybersecurity incident checklist and a sample vendor assessment, according to *Legaltech News*. The guide covers everything from basic security for computer networks to cost-effective approaches to securing computer systems without the burden of additional regulatory requirements.

The second guide, "Cyber Incident Management Planning Guide," focuses more narrowly on actions to take when a breach occurs. The 29-page document examines the five stages of cybersecurity incident management – plan and prepare, detect and report, assess and decide, respond, and post-incident activity – in addition to the current state of information sharing and breach reporting requirements.

According to the IIROC, the guide provides a framework for developing a plan but is not "intended to function as a working response plan. Rather, each dealer member should develop internal plans as part of their cybersecurity strategy that prepares them in advance for the risks they are most likely to face."

"Active management of cyber risk is critical to the stability of IIROC-regulated firms, the integrity of Canadian capital markets, and the protection of investors," said Andrew Kriegler, IIROC president and CEO, in a statement. "That is why we consulted with the industry, engaged security experts and developed concrete resources to help firms better manage their cyber risks."

The IIROC also noted that it is developing a cybersecurity program to help dealers increase their cybersecurity preparedness. In December, the Canadian government announced plans to launch the Canadian Cyber Threat Exchange in 2016, *Legaltech News* reported. It will be an independent, not-for-profit organization to help businesses protect themselves against attacks through information sharing. Its founding members are Air Canada, Bell Canada, Canadian National Railway Company, HydroOne, Manulife, Royal Bank of Canada, TELUS, TD Bank Group, and TransCanada Corp.

INFO SECURITY

Data Breaches Affect U.S. Consumer Business Decisions

Just how much do U.S. consumers pay attention to data breaches? Enough to consider a company's record before choosing to give it their personal information, a recent survey reveals.

Law firm Morrison & Foerster released "Morrison & Foerster Insights: Consumer Outlook on Privacy," which asked consumers about their attitudes on privacy and data breaches. According to the findings, more than one-in-three U.S. consumers (35%) have made a decision whether to purchase a product from a company because of privacy concerns during the past 12 months. In addition, of those consumers that identified themselves as "concerned" about privacy, 82% said that privacy has adversely affected purchasing a product or service, an increase of 28% from 2011.

However, the survey found that just 22% of consumers have stopped purchasing products or services from a company because of a data breach. But it did find that higher-income and higher-educated consumers are more likely to stop purchasing after a breach.

TICK, TOCK... Every Second Counts

"YOUR SCANNER IS PROBABLY JUST TOO FAST."

There, I said it. Your scanner is either too fast, or you don't have enough preppers. That's why it sits there waiting for work.

How fast a scanner feeds paper doesn't really tell the whole story. If we only looked at the scanner's ability to quickly scan documents, we might surmise that a scanner twice as fast would be twice as beneficial. Makes sense, right? Not so fast! (Pun intended!)

WE KNOW THE DEVIL IS IN THE DETAILS

You've heard it many times, the devil is in the details. And in the case of document scanning…the devil is document prep. Document prep refers to that "necessary process" of making paper documents ready to run through a scanner. Take a look on the old InterWeb at the plethora of instructional videos and PDFs touting the importance of prepping your documents properly. They all detail the steps involved in prepping a banker's box full of folders and archived records of one type or another.

Years ago, we identified over 20 different types of prep activities that may occur while documents are being prepared for scanning. For example: Picture a prepper sitting close to a photocopier, surrounded by rolls and rolls of Scotch tape, with blank 8.5 x 11 sheets of paper and patch sheets in hand.

Thus begins the tedious process of removing staples and paperclips, taping torn documents, photocopying delicate or raggedy pages, securing small or odd shaped pages onto larger ones, unfolding and removing creases from pages, inserting document separators, etc. In addition to these steps, there are a number of other activities dedicated to making the paper easier to feed into a high speed scanner. This time-consuming and monotonous process has been widely accepted as the cost of doing business.

We've heard directly from our customers time and again who verify these industry reports that document prep labor accounts for upwards of 70% of the cost of document scanning.

Heck, even our competitors have had to concede what we've been saying for years: Prep kills profits.

EVERY SECOND COUNTS

So, let's say you are looking at one of those high-priced 6000 DPH (documents per hour) scanners. It doesn't really matter how fast it can scan; it matters how long that scanner operator has to wait for the work to be prepped.

It matters how many hours of front-end labor is required to feed the beast. We have found on average that a great prepper can prep a box of files and documents between 750 and 1000 docs per hour. Some preppers are better, some, well…not so much. Efficient document scanning operations, it should be noted, have squeezed as much time as they can out of the process by eliminating a second here, a couple seconds there. In a box of 2,500 to 3,000 documents, those seconds can really add up, and we applaud the effort.

BUT WHAT IF IT WERE POSSIBLE TO CUT OUT EVEN MORE TIME FROM THE PREP PROCESS?

In March of 2015, OPEX customer, BMI Imaging, installed one Falcon workstation in their Sacramento scanning facility. The results exceeded their expectations. BMI was able to reduce its cost of doc prep labor by 30% per box without sacrificing accuracy or quality. The addition of Falcon led directly to several new projects for BMI's clients who had restricted budgets.

With Falcon, BMI can attack more document scanning jobs than ever before. "We are now able to offer more affordable document scanning services to clients with challenging document preparation work," states Whitney. "Our customers are benefiting from both lower prices and higher quality images."

OPEX PREP-REDUCING SCANNERS

Our scanners provide additional business opportunities and the flexibility to:

- Identify and aggressively bid projects with more challenging paper, or more recurring-revenue transactional work (we have thousands of scanners in the field capturing transactional documents);
- Decrease prep headcount, or increase output using the same number of people; and
- Increase your profit margin.

Now that makes sense.

OPEX CORPORATION

CLOUD

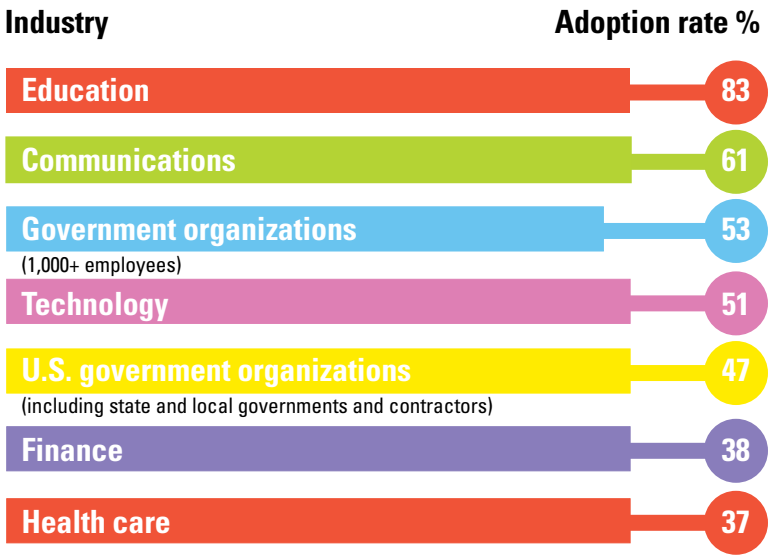
Cloud Adoption Up Across All Industries, Survey Shows

While cloud adoption has significantly increased across all industries, a recent report from data security firm Bitglass revealed that regulated industries are increasingly adopting the cloud. In those industries, adoption jumped from 15% in 2014 to 39% in 2015, with adoption in unregulated industries increasing from 26% in 2014 to 50% last year.

Even heavily regulated industries are increasingly moving to the cloud, the survey shows. Security has always been a concern for these industries; however, the report states that cloud access security brokers (CASB) are filling that gap and enabling widespread adoption of cloud apps across all industries. CASBs offer data-centric security solutions, enabling firms in heavily regulated industries to remain compliant while using public cloud apps, easing the shift away from onsite apps, according to *Legaltech News*.

"Regulated industries have stricter policies in handling sensitive content like personal health information (PHI) and personally identifiable information (PII). Encryption plays a big role in keeping sensitive content from falling into the wrong hands. Traditional cloud solutions do not offer a way to manage and control encryption keys that on-premise solutions offer," Kunal Rupani, principal product manager at Accellion, told *Legaltech News*.

Which industries are racing to the cloud?



Source: Bitglass

Another survey, from Ovum research, revealed that cloud computing adoption is expected to increase over the next decade. A clear majority – 58% – of respondents said they trust the cloud for all business operations. About 78% of survey respondents said they plan to use cloud and software as a service-based applications over the next three years, even for storing and sharing sensitive and regulated data.

Ovum found that data protection is driving cloud adoption because organizations often have limited resources to apply the right data protection to regulated and sensitive data or to prove adequate compliance if the data is stored onsite.

With all that in mind, Ovum says the greatest obstacle facing organizations, lawmakers, and lawyers going forward will be regulating cloud-held data while trying to balance privacy with access and productivity.

Also, the survey found the "most challenging e-discovery environments" may be in South Korea or China, "which have undeveloped or very restrictive climates."

GOVERNMENT RECORDS

NYC Mayor Issues E-Records Directive

Bill de Blasio, New York City's mayor, has issued an executive order to establish standards for proper electronic records management for city agencies through the Department of Records and Information Services (DORIS). The city of 8.4 million residents needs to dispose of 700,000 boxes of documents by 2017.

"This transition will promote improved performance and transparency," the mayor's directive states. "It will be one component of a sensible, comprehensive and compliant information governance program."

'The mayor's directive includes the following guidelines:

- Ensure the preservation of records that have continuing administrative, fiscal, legal, and historical or research value
- Make possible the useful processing of information
- Reduce records storage, equipment, and litigation costs, as well as the costs of other city resources
- Improve operations by documenting agency actions and decisions
- Engage all agency staff in uniform records management practices
- Facilitate access to information in the most efficient manner and at the lowest possible cost
- Ensure agencies operate effectively by appropriately disposing of records that have no archival and minimal value to the city

According to *Politico New York*, the city is currently scanning "millions of papers that are stashed in dusty boxes in private warehouses throughout the city and in New Jersey." The collection totals 2.8 million boxes that will be destroyed.

Half of those are from mayoral agencies, *Politico New York* said, and the other half contains records kept by district attorneys and courts. The DORIS Commissioner's office said it is focusing only on 1.4 million municipal boxes for now. Determining how to digitize the law-and-order papers is a more complicated task. To begin, the city will get rid of boxes containing papers whose required retention periods have expired. There are 169,113 that fall into that category, the agency said.

If the city can get rid of all 700,000 boxes of records by 2017, it estimates it will save $9 million annually in rental costs for records storage.

RIM SERVICES

Iron Mountain/Recall Merger Faces Scrutiny in UK

The Competition and Markets Authority (CMA), the UK's primary competition and consumer authority, said it will investigate Iron Mountain's acquisition of Recall.

Because the companies together provide a large majority of records management and physical offsite data protection services available nationally, the CMA said consumers are worried about loss of competition and choice if the merger goes through. The two companies operate from a total of 59 sites across the UK.

According to the CMA, the merger will be subject to an in-depth phase 2 investigation by an independent group of CMA panel members unless Iron Mountain is able to offer evidence that reduces the competition concerns.

Andrea Coscelli, executive director, markets and mergers, and decision-maker in this case, said:

"Our research and customer responses indicate that these are close competitors in providing 2 distinct types of records and information management services. Iron Mountain is the market leader in both of these markets in the UK. With limited existing competition and no potential new entrants identified, the concern is that the merged company could raise prices or otherwise downgrade those elements of their services which matter to customers."

RIM SERVICES

Microsoft Looks Under the Sea for Future Data Centers

Microsoft researchers believe the future of data centers may lie underwater.

The company said it has tested a prototype of a self-contained data center that can operate hundreds of feet below the surface of the ocean. Because the temperature is chilly down there, the move eliminates an expensive air-conditioning bill, one of the technology industry's biggest obstacles, according to the *New York Times*.

Modern data centers hold thousands of computer servers that create tons of heat. When there is too much heat, the servers will crash. Putting the equipment under cold ocean water could answer the growing energy demands of the computing world because Microsoft is working on placing the system with either a turbine or a tidal energy system to generate electricity, the *Times* said.

The project is code-named "Project Natick," and it might require strands of giant steel tubes linked by fiber optic cables to be placed on the seafloor. Or, Microsoft may suspend jelly bean-shaped server containers beneath the surface to capture the ocean current with turbines that generate electricity, according to the *Times*.

It may sound far-fetched, but researchers believe they could reduce the expense and the deployment time of new data centers from the two years it now requires to just 90 days by mass producing the underwater server containers.

According to the *Times*, the containers could also help speed up web services. Most people now live in urban centers close to oceans but far from data centers, which are usually built in places with lots of space. If servers are placed near users, the delay is reduced.

Microsoft recently conducted a 105-day test of a steel capsule – eight feet in diameter – that was placed 30 feet underwater in the Pacific Ocean off the Central California coast, the *Times* reported. The underwater system, which was controlled from the Microsoft campus in Redmond, Wash., was outfitted with 100 different sensors to measure pressure, humidity, motion, and other conditions in order to learn about operating in an environment where a repairman cannot venture easily or quickly. The new undersea capsules and servers inside are designed to work without needing repairs for as long as five years.

The trial was successful, and the *Times* reported that the research group has started work on an underwater system that will be three times as large. It will be built in collaboration with a developer of an ocean-based alternative-energy system. The developer has not yet been chosen. Microsoft engineers told the *Times* that a new trial will begin next year, possibly near Florida or in Northern Europe, where there are extensive ocean energy projects underway.

According to the *Times*, Microsoft manages more than 100 data centers worldwide, including a more than $15 billion global data center system that now provides more than 200 online services.

CYBERSECURITY

Cyber Attacks on Business Rising

In 2015, 58% of corporate computers had at least one attempted malware attack blocked, up 3% from 2014, according to Kaspersky Lab's Security Bulletin 2015. In addition, file antivirus detection was triggered on 41% of computers or removable media connected to the computers, such as USB sticks or telephones.

E-DISCOVERY

Canada's Information Commissioners Call for a Duty to Document

Canada's information commissioners have asked their respective governments to create a legislated requirement for public entities to document issues related to their deliberations, actions, and decisions.

In a joint resolution, information commissioners expressed concerns about the trend of no records responses for access to information requests. According to the resolution, this weakens Canadians' right of access and the accountability framework that is the foundation of Canada's access to information laws. Without adequate records, it is also difficult for public entities to make evidence-based decisions, fulfill legal obligations, and preserve historical records.

Canada's information commissioners have urged governments to create a positive duty for public servants and officials to create full and accurate records of their business activities. They said this duty must include effective oversight and enforcement that ensure the right of access to public records remains meaningful and effective.

The resolution is available on the websites of the Office of the Information Commissioner of Canada (*www.oic-ci.gc.ca*) and the Office of the Information and Privacy Commissioner for British Columbia (*www.oipc.bc.ca*).

PRIVACY

Survey: New Data Privacy Rules Expected to Cost Companies

A recent Ovum global survey of 366 IT leaders revealed that about 52% of respondents believe the new European Union (EU) General Data Protection Regulation (GDPR) will result in business fines for their company, and two-thirds expect it to force changes in their European business strategy.

Respondents – 63% – also said they think the GDPR regulations will make it harder for U.S. companies to compete, and 70% said the new legislation will favor European-based businesses. Interestingly, respondents cited the United States as the least-trusted country for respecting privacy rights, followed by China and Russia.

More than 70% of respondents expect an increase in spending in order to meet data sovereignty requirements, and more than 30% expect budgets to rise by more than 10% over the next two years as a result of EU regulations. Fines for GDPR violations are potentially 2% of global revenue, which could translate into billions for the world's most profitable companies.

To adapt to the new regulations, 55% of those surveyed said they are planning new training for employees, 51% said they will amend and adapt policies, and 53% said they will prepare by adopting new technologies. Of those who plan to update data privacy strategies in the next three years, 38% plan to hire subject matter experts, and 27% said they will hire a chief privacy officer.

Apparently, such measures are needed: The survey also found that many organizations fall short when it comes to even basic measures to protect data and meet current compliance requirements. For example, just 44% of respondents monitor user activity and use policy-based triggers and alerts. Only 62% have adopted role-based access controls. A little more than 50% actually classify information assets to facilitate controls. Only 54% said they disable PC features, such as external attached drives, while only 57% block access to ungoverned consumer storage and file-sharing apps, such as Dropbox.

The Ovum report recommends organizations conduct a privacy risk assessment, educate their workforces, and ask vendors questions about logical and physical data location as well as service contracts.

INFO SECURITY

Personal Clouds Can Present Security Problems

In an age in which employees can "bring their own cloud" (BYOC) to the workplace, efforts to protect an organization's proprietary information can be challenging.

In a recent action, *PrimePay v. Barnes*, the plaintiff filed a trade secret misappropriation suit against one of its former executives (Barnes) who had established a competing business. The plaintiff sought a preliminary injunction against the operation of Barnes' business, arguing that he had taken confidential company information and stored it in Dropbox.

The plaintiff argued that Barnes used the Dropbox-stored data to help start his new company and then destroyed the materials after the plaintiff warned him "to preserve any PrimePay electronically stored information that he possessed."

The court rejected the plaintiff's argument because Barnes' Dropbox account fell under the company-approved BYOC policy:

"Barnes created the Dropbox [account] … so that he could transfer and access files when he worked remotely on PrimePay matters if he was away from the office, on vacation, or elsewhere and needed access to the PrimePay files, all with the knowledge and approval of [PrimePay owner] Chris Tobin."

Dropbox was a company-approved BYOC provider and, considering factors that suggested Barnes did not access the Dropbox files after leaving his employment with PrimePay, the court found no evidence of trade secret misappropriation and did not issue a preliminary injunction against the operation of Barnes' company. The court did, however, order the destruction of the plaintiff's remaining confidential information that was stored on the Dropbox account.

The decision highlights the importance of developing solid BYOC policies to secure proprietary information and protect other corporate interests. Policies that allow for the use of personal clouds should:

- Clearly describe and define what data can or cannot be transferred to the cloud
- Include audit and enforcement mechanisms to gauge policy observance and disciplinary measures for noncompliance
- Define the nature and extent of the company's right to access, retain, and/or destroy data on a personal cloud for information governance purposes
- Delineate the organization's right to disable a BYOC account either during or after employment
- Outline any employee privacy rights in the data stored in the cloud

GOVERNMENT RECORDS

Ontario: New Fine for Destroying Govt. Records

Anyone caught intentionally altering, concealing, or destroying Ontario government records now will be fined up to $5,000 (Cdn.). Amendments to Freedom of Information and Protection of Privacy legislation at the provincial and municipal levels will require a government organization to develop, document, and preserve its records, according to *The Toronto Sun*.

"Our government takes our record-keeping obligations very seriously we're committed to being open, accountable and transparent," Lauren Souch, a spokesman for Government and Consumer Services Minister David Orazietti, said in an e-mail to the *Sun*. "We promised to open up the government completely, and we have done so to an unprecedented degree."

Organizations that must follow the new rules include government ministries, hospitals, colleges, universities, school boards, municipalities, and police service boards, Souch said.

The penalty comes in response to a concern raised by former Information and Privacy Commissioner Ann Cavoukian that there were no consequences in provincial legislation for the willful destruction of public records, the *Sun* reported. Cavoukian said there had been widespread deletion of e-mails by political staffers as a legislative committee sought records that would have provided more insight into the government's reasons for cancelling gas plants in Mississauga and Oakville at a cost of up to $1.1 billion, according to the *Sun*. Two former senior political aides were charged but have denied wrongdoing.

GOVERNMENT RECORDS

U.S. FOIA Complaints Rise

U.S. President Barack Obama has been quoted as saying he has led the "most transparent administration in history." But in the past two years, the federal government has received more complaints than ever for not fulfilling public record requests, according to analysis by Syracuse University.

Syracuse found that individuals have filed record numbers of federal lawsuits in 2014-2015 – 64% more than the previous two years – against government agencies for failing to comply with requests made under the Freedom of Information Act (FOIA).

Seven years ago, shortly after taking office, Obama issued a memo stating that the FOIA "should be administered with a clear presumption: In the face of doubt, openness prevails."

Former U.S. Attorney General Eric Holder directed agency and department heads to operate under a presumption of openness.

"I would like to emphasize that responsibility for effective FOIA administration belongs to all of us — it is not merely a task assigned to an agency's FOIA staff," Holder wrote at the time. "We all must do our part to ensure open government."

GOVERNMENT RECORDS

Committee Report: 'FOIA Process Is Broken'

A recent majority staff report from the U.S. House Oversight and Government Reform Committee criticized the current administration and several government agencies for undermining the Freedom of Information Act (FOIA).

"The FOIA process is broken," the report states. "Hundreds of thousands of requests are made each year, and hundreds of thousands of requests are backlogged, marked with inappropriate redactions, or otherwise denied."

According to the report, many agencies are lacking transparency when it comes to the FOIA process by adopting an "unlawful presumption in favor of secrecy" when responding to requests. In some cases, huge sections of information that should have been made public – or were already publicly available – were inappropriately redacted, *FCW.com* reported.

The report cites an investigation by the State Department's inspector general that says the department did not search for e-mail records "as a matter of course." According to the report, "The periodic search for emails was only conducted if a request explicitly referred to 'emails' or 'all records.'"

The 39-page report also says the Justice Department and other federal agencies are contributing to the backlog problem by subjecting requests for politically "problematic or embarrassing" records to an additional layer of review, according to the *Wall Street Journal*.

Some lawmakers criticized the report, blaming GOP budget cuts for the FOIA backlog and noted that previous administrations have not always been transparent.

The report calls for structural reform and new legislation to help move the FOIA process toward greater government transparency.

Lawmakers are trying to strengthen FOIA, which is more than 50 years old. The FOIA Improvement Act of 2015, sponsored by Rep. Darrell Issa (R-Calif.) and Rep. Elijah Cummings (D-Md.), passed the Senate Judiciary Committee in February 2015. Among other things, the bipartisan bill seeks to expand the automatic electronic release of documents that receive multiple FOIA requests and allow for consequences for agencies that miss deadlines, *FCW.com* reported.

According to UPI news, the House of Representatives recently passed the FOIA Oversight and Implementation Act, which calls for creating a single online portal for making FOIA requests. It would limit exemptions that allow federal agencies to withhold information and would require agencies to publicly post frequently requested records online.

In addition, according to UPI, the changes would clarify language allowing agencies to withhold information requested only when there is "foreseeable harm" to an interest protected by a FOIA exemption, such as privacy and national security.

PRIVACY

EU Approves New Data Protection Rules

The Securities and Exchange CoIn December, the European Commission (EC) approved the final version of the General Data Protection Regulation (GDPR). The European Union (EU) Parliament was to authorize it early this year, and it will become law for all 28 member states in 2018.

The new rules usurp the EU's 1995 data protection rules (Directive 95/46/EC). The EC has been working on the GDPR since 2012 to strengthen online privacy rights and boost Europe's digital economy.

Experts say GDPR is the most stringent data privacy regulation yet. The new rules apply extraterritorially and so will impact every entity (data processor or data controller) that holds or uses Europeans' personal data both inside and outside of Europe, according to legal experts.

"GDPR is a paradigm change in the way that data collection and use is regulated. We have moved from an era of relatively laissez-faire regulation of data in Europe to having the most stringent data laws in the world," Ross McKean, partner at law firm Olswang, told *ComputerWeekly.com*.

Key provisions of the GDPR include:

- Instituting more rigorous requirements for obtaining consent for collecting personal data
- Raising the age of consent for collecting an individual's data from 13 to 16 years old
- Memorializing the "right to be forgotten," meaning entities must delete data if it meets the specified criteria
- Requiring entities to notify EU regulators of data breaches within 72 hours of the breach
- Requiring entities that handle large amounts of sensitive data to appoint a data protection officer
- Allowing fines of up to €20 million or 4% of a company's global revenue for non-compliance

According to the *National Law Review*, the most significant change brought about by the GDPR is that jurisdiction is not a physical or geographical barrier because it is now digital, meaning that companies outside the EU will be affected by these new regulations if they collect data that belongs to an EU citizen.

"The GDPR looks to adopt prescriptive rules around how organizations will need to demonstrate that they comply with the GDPR," Vinod Bange, partner and head of the UK data protection/privacy practice at law firm Taylor Wessing, told *ComputerWeekly.com*. "Businesses will have to genuinely adopt governance and accountability standards and not pay lip service to data privacy obligations otherwise they could be in for a surprise as the stiff new fines will apply to that requirement too."

Experts say complying with the new rules will require companies to take steps that include mapping and classifying all personal data; performing risk assessments; designing privacy protections into all new business practices; employing dedicated data protection officers; monitoring and auditing compliance; and documenting everything they do with data and everything done to comply with the GDPR, *ComputerWeekly.com* reported.

Eduardo Ustaran, partner and European head of data protection at law firm Hogan Lovells, told *ComputerWeekly.com* that the GDPR features many requirements to make businesses more accountable for their data practices. "This is the area where the heavy weight of the GDPR will be most felt in practice," he said. "New responsibilities such as data protection by design, data protection by default, recordkeeping obligations, data protection impact assessments, and prior consultation with data protection authorities in high-risk cases will require managerial effort and investment."

In the absence of a new Safe Harbor rule, the GDPR does recognize standard contractual clauses and binding corporate rules as legitimate frameworks for transferring EU citizen data out of the EU.

Key provisions of the GDPR can be found at: *https://edri.org/files/GDPR-key-issues-explained.pdf* and *http://www.twobirds.com/en/practice-areas/privacy-and-data-protection/eu-framework-revision*.

E-DISCOVERY

IRS Erased Hard Drive, Spurning Court Order

Despite a court order, the U.S. Internal Revenue Service (IRS) erased a hard drive belonging to a former top official involved in the agency's much-criticized hiring of law firm Quinn Emanuel Urquhart & Sullivan LLP.

Although a litigation hold had been placed on all materials related to the IRS hiring of the outside firm, the hard drive was erased anyway. The order came in response to a Freedom of Information Act (FOIA) request submitted by Microsoft on the IRS contract with Quinn Emanuel.

According to *Law360*'s report, the IRS informed the U.S. Department of Justice (DOJ) in December that it wiped the hard drive in April 2015, after the hold was in place, according to a filing by the DOJ in a Washington federal court. The hard drive belonged to Samuel Maruca, former director of transfer pricing operations at the IRS Large Business and International Division, who helped hire the law firm.

Quinn Emanuel was apparently hired to pursue Microsoft. Even though it had no prior experience handling sensitive tax data, the outside firm was hired at more than $1,000 an hour, according to court records. The initial contract for work was $2.2 million, *Law360* found.

The hiring decision prompted a probe by Finance Committee Chairman Orrin Hatch (R-Utah), who wrote a letter to the IRS stating that hiring outside contractors was expensive and unnecessary, as the agency already employs about 40,000 people responsible for enforcing tax laws. A federal judge has called the decision "troubling."

It's not the first instance of the IRS failing to preserve critical information. The agency also "accidentally" erased the hard drive belonging to Lois Lerner during investigations into the targeting of conservative organizations. As many as 24,000 e-mails were lost when 422 backup tapes were wiped clean despite an agency-wide preservation order and congressional subpoena. In that case, a report by the House Oversight Committee found that the IRS failed to take simple steps to ensure compliance with the order.

COURT CASE

Agencies Must Manage E-mails by End of Year

By Dec. 16, 2016, all federal agencies are required by the Obama administration's information management policy to manage all government e-mail that qualifies as permanent or temporary records in electronic format.

That means agencies must have in place a method of retaining e-mail records in an electronic system that allows for managing and retrieving records and supports litigation needs, open-government requests, and other archival purposes, according to *FCW*.

According to a report released in December 2015 by the National Archives and Records Administration (NARA), 93% of records managers who reported said they are on track to meet the deadline. NARA said it received 84 reports, for a compliance rate of 94%.

"At this point, we're not aware of any agencies that definitively will not make it," Laurence Brewer, NARA's acting chief records officer, told *FCW*. "The 2016 target is an important one. We do expect all agencies to meet that target. But we do realize that it may not be realistic for 100% of agencies given the complexities of their email systems [and] funding priorities, and of course, now we have a presidential transition that's looming."

Brewer said nearly 80% of agencies "report that they have policies and procedures to manage their email." A majority told NARA they plan to implement the agency's Capstone approach to e-mail management, which identifies accounts of key senior officials and key job functions for automatic preservation, *FCW* reported.

The approach is designed to take some of the guesswork out of e-mail management and nudge agencies toward greater levels of automation. Another goal is to eliminate old-fashioned practices such as manually dragging selected e-mails into folders for preservation.

FCW reported that NARA officials plan to release more detailed criteria soon to tell agencies specifically what they need to do to meet the target. In the meantime, NARA is trying to meet its own targets. A 2014 update to federal records laws gave the agency new oversight and inspection authority. To that end, the Office of the Chief Records Officer has grown and reorganized, and NARA has hired more employees with the technical knowledge to help agency records officers manage e-mail systems. **END**