Information Management

PRIVACY

Congress, White House Opt To Kill Broadband Privacy Rules

On March 28, the U.S. House of Representatives voted to kill broadband privacy rules that would have required Internet service providers (ISPs) to get permission from consumers before collecting their sensitive data.

The Broadband Consumer Privacy Rules was approved by a vote of 215-205 that fell largely on party lines, with the Republican majority supporting the motion.

The previous week, the U.S. Senate approved the bill on a similar party-line basis. In April, President Trump signed the bill into law.

The Broadband Consumer Privacy Rules will roll back the legislation passed in October by the Federal Communications Commission that would have given consumers more control over how ISPs can use their sensitive data.

The policy defined sensitive data as any information related to a user's finances, health, information from children, precise geolocation data, web browsing history, and app usage history. ISPs could still collect information not considered to be sensitive, but they would have had to offer customers the ability to opt out of the collection practices.

Additionally, the Broadband Consumer Privacy Rules would have established new requirements for ISPs to report data breaches that may have harmed consumers or put their information at risk. They would have been required to notify customers of a data breach within 30 days of identifying it.

The protections for user data were scheduled for implementation in December 2017. The stricter rules for data breaches were set to go into effect in March, but the FCC under Trump appointee Ajit Pai chose to place a stay on the rules.

GOVERNMENT RECORDS

Legislation Would Strengthen Federal Recordkeeping Requirements

As noted recently on *FedWeek.com,* a U.S. House bill to strengthen recordkeeping requirements for federal agencies has been reintroduced. The Federal Records Modernization Act of 2017, HR-745, introduced by Rep. Mark Meadows (R-NC), would mandate, in part, that agencies capture, retain, and make searchable any electronic messages that qualify as federal records.

The act would also modify the categories of record removal or destruction that require agency chiefs to notify the National Archives and Records Administration (NARA) and begin actions to recover removed records through the Department of Justice. Federal agencies would also have to apprise NARA of any falsifications of records or concealments and publish a description of records that have been lost or are at risk of being lost.

HR-745 also establishes a process for suspending and removing employees if an agency inspector general deems they have "willfully and unlawfully concealed, removed, mutilated, obliterated, falsified, or destroyed any record, proceeding, or other thing in their custody" or have violated prohibitions against sending or creating records via unofficial messaging accounts.

The bill, which was referred to the House Committee on Oversight and Government Reform, would also require agencies to tap a senior records management official to be responsible for ensuring compliance with records management requirements.

E-MAIL

Minn. Agencies Resist Efforts to Clarify E-mail Retention Rules

State Representative Peggy Scott, a Republican from Andover, Minn., recently introduced a bill that would require state government agencies to save public electronic communications for at least three years, as recommended by a state records retention panel. The legislation would clarify a law that does not provide detailed guidelines for retaining information not considered "official" records.

According to a recent article on *MinnPost.com*, the effort has met with opposition from state agencies, who claim the bill would be a burden. The debate has veered into related topics as well, including government transparency and the value of historical documents.

Some agencies have set up their own e-mail retention timelines, deleting e-mails at their discretion. It is legal for them to do so; state law only requires government to save and make public records that are part of an "official action" or "in connection with the transaction of public business."

That language has been interpreted in many ways. For example, the Hennepin County Sheriff's office recently changed its e-mail retention policy to automatic deletion after 30 days. The county itself is shifting to a six-month e-mail retention policy, after which e-mails will be automatically deleted.

Scott argues those e-mails are an important piece of how government operates and are critical if agencies want to remain transparent. She wants to set up a uniform system across government agencies, eliminating the word "official" from state law to open up the number of records that must be saved.

Some worry that history is being destroyed in the deletion of e-mails.

"Keeping our history, that's what we're talking about," said Don

Gemberling, former director of the Information Policy Analysis Division. "If you wanted to go to a library and look at history you would be able to find a number of correspondence between people. Currently, much of that correspondence is in emails, and if government is allowed to get rid of emails, and frankly, a lot of other electronic records, we're going to lose something really important."

Scott's bill has no direct companion in the state Senate, and a similar bill to require government agencies to save their e-mails for at least 18 months has stalled there.

Some local officials say the three-year e-mail retention policy would require new tools, incur great costs, and spike the staff time required to respond to data requests from attorneys or reporters when so many records are required to be kept on file.

INFO SECURITY

DHS Committee Approves Breach Notification Best Practices

In February, a U.S. Department of Homeland Security (DHS) advisory committee approved a set of best practices for DHS agencies that may someday have to notify employees or clients of a data breach.

According to *NextGov.com,* the action may stem from the data breach that struck the Office of Personnel Management in 2015, possibly affecting some 20 million current and former federal employees and their families.

The best practices document encourages agencies to seek a balance in their notification procedures by moving fast enough to comply with legal requirements and to give people time to take defensive measures, but not so quickly as to provide confusing or false information. It cites the danger of "over-notification," which could result in people not taking the notices seriously.

The DHS Data Privacy and Integrity Advisory Committee added language that would help the recipients verify that the notice itself was not a phishing scam and to ensure all notices are accessible to those with disabilities or who don't speak English.

The document follows guidelines established by several federal agencies and a formal guidance document from the Office of Management and Budget that was released in January.

INFO SECURITY

Australia Passes Data Breach Notification Law

As reported in several outlets, after years of failed attempts the Australian legislature has passed the country's first mandatory data breach notification law. The law will apply only to companies with more than $2.3 million in annual revenue and will require covered entities to notify the Australian privacy commissioner and affected individuals of certain data breaches. Overseas companies are subject to the law when they hold information on behalf of a covered entity.

The law will apply only to what it defines as "eligible" breaches – those where a reasonable person would conclude there is a risk of "serious harm" to an affected individual after the unauthorized access or disclosure of personal information.

An explanatory memorandum accompanying the legislation explains

that serious harm "could include serious physical, psychological, emotional, economic, and financial harm," while only being distressed is not enough to constitute an actionable breach. According to the law, notice is not required if the company takes action to stop serious harm before it occurs.

The law will be enforced by the privacy commissioner, who is authorized to seek civil penalties of up to $1.8 million and can require offending companies to take remedial steps. The law is expected to become effective next year, although an exact date has not been announced.

Australian Privacy and Information Commissioner Timothy Pilgrim recently issued an official statement welcoming the passage of the *Privacy Amendment (Notifiable Data Breaches) Bill* 2016.

Pilgrim said his office will work with those organizations to ensure they are prepared for when the law is implemented.

"The new scheme will strengthen the protections afforded to everyone's personal information, and will improve transparency in the way that the public and private sectors respond to serious data breaches," Pilgrim said in the statement. "It will also give individuals the opportunity to take steps to minimize the damage that can result from unauthorized use of their personal information."

Pilgrim said his office received 107 voluntary breach notifications in 2015-16.

PRIVACY

Japan Privacy Law to Change on May 30

Revisions to Japan's Act on the Protection of Personal Information (APPI), combined with the start-up of a Personal Information Protection Commission (PPC), likely will affect the international community's cross-border data transfers with Japan.

As summarized on *Lexology.com,* PPC Director Yoshikazu Okamoto spoke in a presentation in Washington about these key aspects of the amended APPI, one of Asia's oldest privacy laws, which was established in 2003:

- The PPC will have centralized data protection authority over all ministries. It consists of a chairman and eight commissioners appointed by the prime minister, with consent of the Diet (Japan's legislature).
- Consent will be required to use or disclose "special care-required personal information," which includes data about a person's race, creed, social status, medical record, criminal history, and crime-victim status.
- Consent will not be needed to transfer or process anonymously processed information.
- To improve the traceability of personal information that businesses share, the amended APPI calls for companies to keep records of how or from whom they obtained that information and to whom they transferred it.
- The new APPI lists three types of legitimate transfers of personal information to a third party in another country: 1) transfers to a country the PPC says has an acceptable level of data protection; 2) transfers to a third party in a country that ensures the same level of data protection as Japan; or 3) transfers with the data subject's consent.
- International transfers of personal information can continue if reasonable safeguards are in place.

The amended APPI will take effect on May 30.

Difficult Documents. Simple Solution.

Rapid growth can be a boon for a small company, but it also brings many challenges along with it. With growth comes an increase in volume and demand, and to meet that demand, companies often have to invest in labor, technology, or both.

That certainly was the case at Chicago Records Management, Inc. (CRM). CRM provides document management solutions to a wide range of customers. These solutions include off-site storage, document imaging, and online content management. The company also offers data protection services such as tape vaulting and online back-up capabilities.

On-Site Demo Proves Productivity Increase

OPEX brought a Falcon® scanner to the CRM facility and ran the customer's documents through the scanner on-site. "That test in their facility was the validation we needed to ensure this would be a good platform for their application," said Greg Bank, Senior Account Executive at OPEX.

"If it weren't for the extended on-site demo, and having OPEX put all that time into building the sample jobs and workflow, there is no way I would have considered buying one of these machines," Maiers says. "For a company our size, a significant investment like this would be too much of a gamble without being able to see how it handled our actual workflow.

"At the end of the demo, the staff here who would be working with the machine came to me and said, 'This is awesome,'" Maiers adds. "The numbers we got back on the demo showed we could operate two to three times faster."

Falcon made it much simpler to scan the materials and required less work. "The way that Falcon is designed, it eliminated just about 98 percent of the flatbed scanning we had to do," Maiers says.

Minimize Labor, Maximize Quality

Falcon is a one-touch document scanning workstation that allows operators to scan a broad range of document sizes and formats with minimal labor, which makes it easy for employees at CRM to prepare the marketing documents for imaging. Once Falcon has ingested these documents, the batches of scanned images are converted to PDF files using OPEX Transform™. The PDF files are then forwarded to the customer's proprietary document management solution.

"The client is really focused on image quality and wants their scanned documents in a particular order based on how the mail pieces are typically opened and read," Maiers says. "What Falcon allows us to do to scan the first page then, in rapid succession, manipulate and rotate each subsequent piece so it can be imaged in the manner that it was meant to be read."

Each page is evaluated for image quality, correct order, and orientation as the documents are processed. According to Maiers, the company is scanning roughly 2,500 envelopes/pieces per day for the client.

"It literally scans whatever we throw at it."

Using OPEX Falcon, CRM was able to meet its customer's high-volume imaging needs without adding personnel or increasing costs. Because employees don't have to manipulate the mail pieces before scanning, Maiers says the company is doing three to five times the volume of work per day with less labor. "The Falcon's ability to handle mixed media in an incredibly efficient manner is what makes these machines as valuable to me as they have become. It literally scans whatever we throw at it," says Maiers.

The new Falcon units are more productive than the previous hardware, and Maiers says he can get the same throughput from the system with two employees that he was previously able to achieve with four to six employees using the old solution.

Read the entire article here.

For more information visit *www.opex.com*

OPEX CORPORATION

PRIVACY

E-privacy Directive, GDPR Expected to Take Effect May 2018

Lexology.com recently summarized the European Commission's (EC) new e-privacy regulation, which is expected to replace the current directive from 2002 and be applied throughout the European Union.

The EC expects the regulation to be effective concurrent with the launch of the General Data Protection Regulation (GDPR) in May 2018. The draft of the new regulation is narrower in scope than the GDPR and should not take as long to finalize, according to *Lexology.com*.

The article summarized the key features of the draft regulation:

- *Scope.* The regulation applies to all e-communications service providers, whereas the current law applies only to traditional telecommunications service providers.
- *Confidentiality.* All e-communications must be kept confidential.

- *Communications* content and metadata. Metadata and browsing histories must be anonymized or deleted unless the user gives consent to retain it.
- *Devices.* Data stored in end-user devices, like laptops and tablets, cannot be accessed unless the user gives consent or it is necessary to facilitate technical provisioning of services to that user.
- *Spam.* Consent must be given before any unsolicited commercial communications can be transmitted. Member states can also make rules that allow individuals the right to object to marketing calls.
- *Cookies.* The consent process for Internet users will be simpler with the introduction of levels of privacy through the users' browser settings. The need for banner-type cookie consent is being removed. Cookies that are not intrusive will not require consent.
- *Enforcement.* National data protection authorities will enforce the new regulations. Fines could reach €10 million ($10.7 million U.S.) or 2% of worldwide annual turnover of an undertaking, whichever is higher. Fines of up to €20 million ($21.4 million U.S.) or 4% of worldwide annual turnover could be enforced for breaches of the provisions on confidentiality, processing of e-data, and limits on data erasure periods.

PRIVACY

Dutch Act Proposed for Implementing GDPR

Stibbe.com recently reported on the proposal for a Dutch General Data Protection Regulation (GDPR) Implementation Act that would include a legal framework for implementing the European Union's (EU) GDPR, which goes into effect in May 2018. The Dutch act will supersede the Dutch Data Protection Act, which has been applying EU Directive 95/46/EC.

The GDPR requires EU member states to implement some topics, but the new regulation permits discretion, which has opened the door for the Dutch act. Government in the Netherlands has indicated it will seek "policy-neutral" implementation and follow the current EU Directive as closely as possible, according to *Stibbe.com*.

According to the article, if the implementation act is not further revised, it will cause some changes, including, for example, how appointments are made with supervisory authorities; how officers are appointed to the authorities; and permissions for processing biometric data for the purpose of identifying an individual.

PRIVACY

Gartner Study Finds a 31% Spike in IoT Worldwide

Based on its recent study, research firm Gartner Inc. predicts there will be 8.4 billion Internet of Things (IoT) devices in use worldwide by the end of this year, which represents a 31% spike from the end of 2016, as summarized recently on *NetworkWorld.com*.

The number is expected to keep growing at a similar pace until 2020, when some 20 billion connected devices are expected to be in use, according to Gartner.

Nearly two-thirds of connected products will be consumer items, such as smart TVs, set-top boxes, and automotive devices. Such home items as connected door locks and lightbulbs, though popular with tech-savvy targets, have not yet reached the mass consumer market

Businesses spend more than consumers on IoT products – doling out $964 billion this year, while consumers will spend $725 billion, Gartner predicts. For the business market, vertical industries like health care and manufacturing lead the way with 1.6 billion products, but cross-industry IoT systems, such as connected lighting, heating and security, will likely surpass the vertical uses by next year, according to Peter Middleton, Gartner analyst.

Less expensive products developed in China could fuel an even faster growth in IoT, Middleton believes. China's electric utilities have driven down the cost of smart meters, for instance, and such a competitive-bidding process could swamp the west with cost-effective goods.

There is always the chance that security concerns will cool the consumer's desire for smart products in the home. The 2016 distributed denial of service attack from a botnet of insecure connected cameras and DVRs is expected to have an impact. Said Middleton, "It could cause consumers to think twice about employing connected devices."

CYBERSECURITY

IoT is Easily Hackable Today; EC Hopes to Change That

Lauren Cerulus of Politico recently reported on efforts by the European Commission (EC) to stem the growing threat of denial-of-service attacks on the billions of devices connected to the Internet. Currently, when consumer goods that make up the Internet of Things (IoT) are hacked, their manufacturers face no legal action in Europe because there is no legislation for it.

But after being the victim of a denial-of-service attack last fall, the EC and European Parliament are taking such threats more seriously.

The EC is crafting a "trust label" for IoT products that would inform customers if they're buying something that's hackable. Further, the e-privacy regulation that's working through Parliament could also affect how some products, such as voice-controlled applications, approach their communications data.

According to Cerulus, the EC also hopes to propose legislation on cybersecurity certifications this year to support the voluntary standards that have been put in place by the mobile industry association and other corporate interests. The EC is expected to lay out its latest cybersecurity strategy this summer, updating a 2013 plan that largely predated such threats to the IoT.

All said, it may be years before manufacturers have a distinct set of binding security standards.

Today, few IoT devices ask new owners to change the default login, which leaves that item – a refrigerator, a thermostat, or a security camera, perhaps – vulnerable to intrusion.

"You can blame the users, but that's not fair," said Lori Wigle, a senior manager with Intel. "The device maker can build in a mechanism that triggers users to change [the original login]."

Politico's Cerulus uses the example of the website Insecam, which hosts a database of online security cameras that can be accessed remotely. With just a couple clicks, a hacker could be looking at the back yard of someone who forgot to change his password.

PRIVACY

Privacy Law Changes Coming This Year to Canada

Thanks to Canadian privacy law changes and recent guidance from the Canadian Securities Administrators (CSA), Canadian companies soon will have to start disclosing more about cyberattacks and be more proactive about revealing specific risks that could result in future attacks, according to a report on *CanadianCyberSecurityLaw.com*.

In June 2015, the Canadian government passed the Digital Privacy Act. Among other things, it requires data breach notification and reporting regulations to become part of Canadian privacy law. According to CBC News and an Innovation, Science and Electronic Development spokesperson, the government expects to publish draft regulations "sometime in early 2017," but it has not announced a date when the final regulations will be published or become law. Some in the industry say they expect the regulations to take effect by the fourth quarter of this year.

After that, organizations will be required to report all breaches and notify users of any breach that poses "a real risk or significant harm."

… the hope is that more transparency will lead to better protections and fewer breaches.

According to CBC News, that would include any information that could be used to commit fraud or a social engineering attack. But it could also include information that could humiliate a person or damage his or her reputation.

Companies also will have to reveal more about how they are protecting individuals' data. If data is lost or stolen, companies will have to tell the individual or risk a fine. Failure to report a breach or notify users when required could result in a fine of up to $100,000 (Cdn.; approx. $75,000 U.S.).

Cybersecurity experts say there is a significant number of breaches that never get reported because there's currently no obligation to report them, but that will start to change later this year.

Kevvie Fowler, KPMG's national leader of cyber response in Canada, told CBC News that he expects the number of reported breaches will "skyrocket" this year because of the new regulation. And with more reported breaches, there will be more angry victims, meaning a likely increase in the number of companies being sued, he said.

According to Fowler, the hope is that more transparency will lead to better protections and fewer breaches.

In the meantime, the CSA is working to ensure that publicly traded Canadian companies are more transparent about their cybersecurity practices before they get hacked – and not just after a breach.

According to CBC News, the CSA recently reviewed how 240 publicly traded companies in Canada talked about cybersecurity in their financial filings. The CSA found that 40% of companies failed to address cybersecurity risks in their disclosures. And, in general, it found that filings tend to use generic, boilerplate language, even though different types of companies face different types of cyberattacks or threats and hold different types of data with varying degrees of risk.

In its guidance note, the CSA says it expects issuers "to provide risk disclosure that is as detailed and entity-specific as possible" and that it will be monitoring companies for compliance.

Take Our Latest One-Minute *IM* Poll

We'd like to know how well your RIM program is understood, supported, and valued. Please take a minute to answer a few questions at ***http://imm.exploreamra.org/My_RIM_Program.***

Read the article that prompted this survey on page 38.

See the April 2017 Poll Results for **Where RIM Reports**

More than half of the 468 who had responded by press time said the RIM program reports to one of three functional areas. Of the 15 possible responses, these were the top five answers:

18% – Admin./Business Services
18% – Information Technology
18% – Legal
12% – Other
10% – An Executive Officer

View the full results – or respond to the poll if you haven't already – at ***http://imm.explorearma.org/Where_Does_RIM_Report.***

WEBSITE & REGISTRATION WILL GO LIVE ON OR BEFORE JUNE 1

Your role is changing. Our profession is changing.

How the world uses records and data to make informed decisions and shape policy is changing.

Join ARMA International and hundreds of your peers to learn more about how you can lead the change and move your careers, your organizations, and the world forward.

Agents of Change

ARMA LIVE! ORLANDO

OCTOBER 15-17 | MARRIOTT WORLD CENTER | ORLANDO, FL

INFO SECURITY

IBM, FDA to Help Advance Blockchain for Health Records Management

As reported on *GCN.com,* IBM Watson Health has announced a joint research initiative with the U.S. Food and Drug Administration (FDA) to leverage blockchain technology for the safer, more efficient exchange of healthcare data.

A shared ledger technology that underpins the Bitcoin online currency, blockchain is becoming a building block for how some industries will reshape the way they share, store, and secure information.

The IBM/FDA partnership will soon explore the use of blockchain for exchanging data from e-medical records, clinical trials, genomics, mobile devices, wearables, and Internet of Things devices.

According to an FDA official, blockchain has the potential to support the safe exchange of great volumes of data while ensuring privacy and integrity. Angela Stark, an FDA press officer, said, "These are critical features of a scalable data exchange ecosystem that can support high-quality research while safeguarding against breaches of sensitive patient-level data."

An IBM Watson Health statement said that "Blockchain technology provides a highly secure, decentralized framework for data sharing that will accelerate innovation throughout the industry.

A 2016 Deloitte report supports such views, finding that blockchain technology could transform healthcare's IT infrastructure and increase the security, privacy, and interoperability of health e-records by changing the way the organizations exchange the data.

"The current state of health care records is disjointed and stovepiped due to a lack of common architectures and standards that would allow the safe transfer of sensitive information among stakeholders in the system," said the Deloitte report.

E-DISCOVERY

Judge Fed Up with Lazy Discovery Efforts

Lawyers need to get up to speed on the 2015 rule changes to the U.S. Federal Rules of Civil Procedure (FRCP), according to a U.S. federal magistrate judge in Manhattan.

Southern District Magistrate Andrew Peck said too many attorneys are not adhering to the 2015 revisions to Rule 34 of the FRCP, according to *LegalTechNews.com.* The revisions were designed to speed up responses to discovery requests, clear up objections to requests, and eliminate the confusion that can slow down production.

"It is time, once again, to issue a discovery wake-up call to the bar in this district," Peck wrote in *Fischer v. Forrest,* a Lanham Act trademark infringement case, in which he issued a report and recommendation on motions to dismiss earlier this year.

Peck said Rule 34 requires a litigator to state grounds for objections with specificity; state whether any responsive materials are being withheld on the basis of that objection; and specify the time for production – and, if it's a rolling production, state when production will begin and end.

"Most lawyers who have not changed their 'form file' violate one or more (and often all three) of these changes," he said.

The 2015 Advisory Committee Notes on Rule 34(b)(2)(C) said requiring lawyers to state whether anything is being withheld based on a particular objection "should end the confusion that frequently arises when a producing party states several objections and still produces information, leaving the requesting party uncertain whether any relevant and responsive information has been withheld on the basis of the objections."

Peck is handling discovery in two related cases brought by James Fischer, inventor of "Fischer's Bee-Quick," which is designed to facilitate honey harvesting. Fischer sued the principals of Brushy Mountain Bee Farm Inc. and the company, an authorized dealer of Bee-Quick that was permitted to use Fischer's copyrighted works on its sales website and catalog.

But Fischer said the defendants began in 2011 to market "Natural Honey Harvester," an unauthorized imitation of Bee-Quick.

Peck said that "despite the clarity of the no-longer-new 2015 amendments, this court still sees too many non-compliant Rule 34 responses."

The defendants made 17 "general objections" in their latest Rule 34 response, prompting him to say, "Let us count the ways the defendants have violated the rules."

For instance, a response to two requests stated they were "overly broad and unduly burdensome" – phrases the judge called "meaningless boilerplate."

Peck said anyone who doesn't comply with Rule 34's requirements on specificity and clearly indicate whether material is being withheld based on the objection "will be deemed a waiver of all objections (except as to privilege)."

PRIVACY

Canadians Want Tougher Privacy Laws, Poll Reveals

Canadians want tougher privacy laws, and they want government and businesses to be more upfront about how they collect and use personal data according to a survey commissioned by the Office of the Privacy Commissioner (OPC).

Most Canadians support amendments to the Privacy Act, which covers the personal information-handling practices of federal institutions, the survey revealed. In addition, Canadians widely support requiring government institutions to safeguard the personal information they collect about Canadians (78%) and expanding the Privacy Act to the prime minister's office and cabinet ministers (71%). Another 69% support granting the privacy commissioner order-making power to enforce recommendations made following an investigation, while 66% think government institutions should to assess the privacy risks of any new program or law.

"Canadians agree it's time to

modernize the Privacy Act, which has gone largely unchanged since it was introduced in 1983," said Commissioner Daniel Therrien, who recently proposed amendments that a parliamentary committee largely supported.

In the survey of 1,500 Canadians, 92% were concerned about the protection of their privacy. Nearly two-thirds said they don't know what is being done by government with their personal information and seven in 10 Canadians said intelligence and law enforcement agencies should report publicly on how often they request personal information from telecommunications companies without judicial oversight. Most Canadians (81%) expressed concern about government monitoring for national security reasons, although half said they don't believe the agencies have sufficient powers to collect private information from citizens.

When it comes to business transactions, Canadians support measures that would give them more control over personal information collected online. For example, 86% agree websites should seek their consent for targeted advertising. Given that just four in 10 admitted to reading privacy policies before downloading applications, the OPC's discussions about how to make consent more meaningful are much needed.

Canadians also believe businesses should be more accountable, with seven in 10 saying they would be more willing to do business with companies if they were subject to strict financial penalties for misusing their personal information.

FOIA

ACLU Files 13 Lawsuits For Records Related To Travel Ban

In April, the American Civil Liberties Union announced that its affiliates had filed 13 coordinated Freedom of Information Act lawsuits, demanding government documents related to implementation of the president's executive orders on travel and immigration, as reported on *npr.org.*

The ACLU seeks records from the local offices of U.S. Customs and Border Protection (CBP) and the Department of Homeland Security — records it says it first requested on Feb. 2.

The lawsuits seek information from 13 local CBP offices, mainly in cities with international airports "where there were reports of some kind that we wanted to get information about, and we wanted to get it from the people handling it on the ground," said Gabriela Melendez, political communications manager for the ACLU.

The FOIA requests seek any records on the implementation of the travel bans, including text messages, voicemails, e-mails, contracts, directives, and training documents.

The ACLU says the agency has a long history of not complying with FOIA rules.

Last July, the ACLU sent a letter to then-CBP Commissioner Gil Kerlikowske complaining that often "FOIA requesters receive no response whatsoever. Those who do receive a response are frequently told (erroneously) that no records exist, or they are provided with incomplete responses and/or overbroad and unlawful redactions that are contrary to the FOIA statute, case law, and implementing agency regulations."

In a statement to NPR, ACLU said those frustrations persist under the new administration: "CBP continues to treat the Freedom of Information Act with contempt. CBP routinely fails even to respond to FOIA requests and flouts its transparency obligations by forcing federal court intervention to pry loose information which the public is entitled to."

GOVERNMENT RECORDS

Audit Finds Victoria's Records Management Practices Outdated

Victoria's Public Records Act of 1973 could not have anticipated the changes that would come in the information management landscape. A review of the Management of Public Sector Records conducted by the Victorian auditor-general confirms this view, according to the Australian site Image and Data Manager.

The audit found that Victoria's information management environment is "highly fragmented and disconnected – with multiple sets of policies and standards that can sometimes contradict each other."

The audit noted that the absence of a system-wide compliance monitoring and reporting mechanism heightened the risk of key government records being lost, misused, altered, or unlawfully destroyed. It also acknowledged how the spike in the number of records only intensifies the problems.

"The volume of records created and held by agencies and third-party providers has also increased significantly. At the same time, new business practices and advances in technology have increased the risks relating to information integrity, accessibility, security and preservation."

The auditor-general also examined the records management practices of the Department of Education and Training and the Department of Health and Human Services. Neither agency was found to comply with legislative requirements.

According to the report: "Consequently, neither agency sufficiently understands the records it owns and holds, and cannot be assured that their records are being effectively managed and maintained.

Both agencies, which handle highly sensitive records, were found to have these problems:

- Insufficient authority given to, or applied by, the central records management unit
- Inadequate training for staff, contractors, and consultants on their records management responsibilities

- Little assurance that providers are lawfully managing records
- Insufficient monitoring
- Lack of compliance with the Capture specification, which requires agencies to have records that are authentic, reliable, usable, and trustworthy

In June 2016, the Victorian state government said it would perform a full review of the Public Records Act 1973. The auditor-general's current report is available at *http://www.audit.vic.gov.au/reports_and_publications/latest_reports/2016-17/20170308-public-sector-records.aspx*.

CYBER SECURITY

IRS Student Loan Breach Compromises up to 100,000 Taxpayers

In April, the IRS said the personal data of up to 100,000 U.S. taxpayers could have been compromised through a scheme whereby hackers posed as students using an online tool to apply for financial aid, according to an article in the *New York Times.*

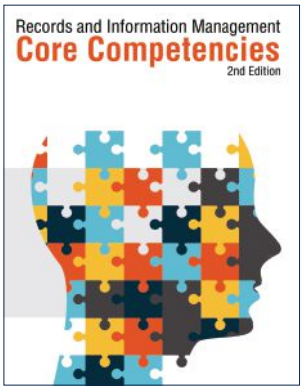
The attack became known in March when the IRS closed its Data Retrieval Tool, which families use to import tax data to the Free Application for Federal Student Aid site, on the Education Department's website. The shutdown occurred at the height of financial aid application season.

The IRS has been struggling to overhaul its defenses against increasingly sophisticated cyberthreats as its budget shrinks and its staff dwindles.

Last fall, the IRS realized criminals could exploit the student loan tool, which allows aid applications to automatically populate with their parents' tax information. The fear was that thieves could use the stolen data to file fraudulent tax returns.

The IRS does not expect the tool to be secure and operational again until October.

New and Free to **ARMA Members!**



Download your free copy of ***Records and Information Management Core Competencies, 2nd Edition*** today at ***www.arma.org/go/prod/V5934***

Not a Member? You should be. **Join Today!**

Invest in yourself by joining the thousands of ARMA members who are boosting their careers with the help of our education, events, publications, and more. Your small investment will pay for itself several times over when you take advantage of just a fraction of the benefits that membership offers. To find out more, visit ***www.arma.org/r1/membership/membership-benefits***

PRIVACY

UK ICO Offers Guidance on the GDPR; Final Draft Expected Soon

In March the UK Information Commissioner's Office ("ICO") published a draft of its guidance for the consent requirements of the EU General Data Protection Regulation (GDPR). The draft describes how the ICO interprets the consent requirements of the GDPR and the recommended approach to complying with it.

Jo Pedder, ICO, point person for the guidance, issued a statement on an ICO blog about the draft and welcomed the public to comment. (The comment period has since closed.)

Pedder wrote of how the GDPR sets a high standard for consent: "It builds on the Data Protection Act (DPA) standard of consent in a number of areas, and it contains significantly more detail on both the standard and processes for consent. Basing your processing of customer data on GDPR-compliant consent means giving individuals genuine choice and ongoing control over how you use their data, and ensuring your organisation is transparent and accountable."

She empahsized that "getting this right" is beneficial to the organizations as well because it's essential to good customer service and will help build confidence and trust: "It's one way to set yourself apart from the competition and will be fundamental to the growth of the digital economy."

Pedder noted that the guidance explains the ICO's recommended approach to compliance and what counts as valid consent. It provides practical help to decide when to rely on consent and when to look at alternatives.

The final draft of the guidance is expected to be published in May.

PRIVACY

VIZIO to Pay Millions for Spying Through Internet-Connected TVs

As reported on *FTC.gov* and other outlets, VIZIO Inc., a manufacturer of smart TVs, has agreed to pay $2.2 million to settle a regulatory complaint that it tracked its consumers on their Internet-connected smart TVs without their consent or knowledge.

The Federal Trade Commission (FTC) said VIZIO collected viewing habits from 11 million devices, beginning in February 2014, using new and previously sold TVs that hadn't shipped with automated content recognition (ACR) software installed. The software periodically added IP addresses to the collected data and made it possible to connect to more detailed information, such as age, sex, marital status, household size, income, and more.

The Office of the New Jersey Attorney General and the FTC alleged that VIZIO tracked what consumers watched on their Internet-connected smart TVs through software the company turned on by default. According to the complaint, VIZIO provided IP addresses and viewing data from TVs to third parties who used the information to analyze the effectiveness of advertising. Regulators said this data was combined with demographic information associated with a consumer or a household and then used by third parties to target advertising.

In an e-mailed statement, VIZIO officials said this: "The ACR program never paired viewing data with personally identifiable information such as name or contact information, and the Commission did not allege or contend otherwise. Instead, as the complaint notes, the practices challenged by the government related only to the use of viewing data in the 'aggregate' to create summary reports measuring viewing audiences or behaviors."

The settlement, in part, says VIZIO must delete any data collected before March 1, 2016, and implement a comprehensive privacy program, subject to biennial assessments by an FTC-approved entity for the next 20 years. VIZIO must also add prominent disclosures and get affirmative consent before collecting and sharing viewing data – separate and apart from any "privacy policy," "terms of use" page, or similar document.

PRIVACY

A PrivacySmorgasbord on Capitol Hill

The past several weeks have seen these privacy-related bills introduced onin the U.S. Congress:

H. R. 2204 – Homeowner Information Privacy Protection Act. This bill would require a study of whether data collection under the Home Mortgage Disclosure Act of 1975 would increase the probability of such things as mortgage applicants' personal identities and data being exposed and the likelihood that the data would be used for marketing or selling unfair, deceptive, or abusive financial products to the applicants.

H.R. 2227 – Modernize Government Information Technology Act. The goal is to modernize federal IT systems and processes to mitigate cost and risk.

H.R. 1868 – Restoring American Privacy Act of 2017. The bill is in response to the April action that halted the enacting of the American Privacy Act of 2017, therefore allowing Internet service providers more freedom to use subscribers' personal data.

S.878 – A bill to establish privacy protections for customers of broadband Internet access service and other telecommunications services. This is the Senate's version of H.R. 1868.

S.877 – Protecting Student Privacy Act of 2017. The bill would amend the Family Educational Rights and Privacy Act of 1974 to ensure that student data handled by private companies is protected.

H.R. 1899 – Protecting Data at the Border Act. The bill would ensure the digital contents of electronic equipment and online accounts belonging to or in the possession of U.S. persons entering or exiting the United States are adequately protected at the border.

CYBERSECURITY

Study Urges Wider DMARC Implementation to Fight Phishing

On March 3, the Federal Trade Commission (FTC) announced the results of a study that looked at the ways online businesses use e-mail authentication to prevent phishing attacks. The sample consisted of 569 online businesses that have ties to the United States.

The study found that most major online companies are using proper e-mail authentication technology to prevent phishing, but few are taking full advantage of the best technologies. Eighty-six percent use Sender Policy Framework, which enables Internet service providers (ISPs) wto see if an e-mail message originates from the domain it claims to.

In a subsequent report, the FTC recommended wider use of DMARC, which stands for Domain Message Authentication Reporting & Conformance. It alerts the company about spoofing efforts and advises the to reject messages that claim to be from the company's e-mail address.

The study found that fewer than 10% of the companies use DMARC.