Information Management

DATA LEGISLATION

CLOUD Act Seen as Compromise Between Big Companies and DoJ

In March, the CLOUD ACT (short for *Clarifying Lawful Overseas Use of Data*) was embedded deeply in the U.S. federal government's $1.3 trillion budget bill, contemporaneous with the Supreme Court's hearing of a long-running case that questions the reach of U.S. law enforcement into the foreign operations of U.S. companies.

According to *FCW.com*, the new law effectively rendered the case of *Microsoft vs. U.S.* moot. Indeed, weeks later, on April 17, the U.S. Supreme Court dropped the case.

Some view the legislation as a compromise because it gives law enforcement a way to obtain data through the subpoena process, but it also provides companies with a means to appeal such requests if compliance would compel them to break local laws.

"This bill is a significant step forward in the larger global debate on what our privacy laws should look like, even if it doesn't go to the highest threshold," said Hasan Ali, Microsoft's senior attorney on national security and law enforcement. "The law

incentivizes [foreign governments] to go and reform their laws, to elevate their standards, and human rights conditions."

An official with the Department of Justice foresees the issue of privacy concerns as states and local jurisdictions get involved. "We may well see state and local warrants that want to use this process in order to obtain compliance from foreign providers, or providers storing data overseas," said Richard Downing, an acting deputy assistant attorney general. "And how exactly that will work is still up in the air."

Additionally, there is concern that foreign governments might be given easier access to U.S. data because the law permits the president to enter into executive agreements with foreign governments covering data collection on criminal suspects.

"We get requests from other countries for investigating crimes that would not be a crime and in fact would be protected speech if it were to occur in the United States," Downing said. Even if a request were impermissible under a Cloud Act agreement, it could move to the Mutual Legal Assistance Treaties process, he said.

Downing also warned that the new law could create a "diplomatic headache" for the United States because there will be countries that could be denied an executive agreement because Congress may not approve.

CYBERCRIME REPORT

Predictably, Symantec's Threat Report Shows Dramatic Increases in Cyber Crime

Symantec's 2018 *Internet Security Threat Report* confirms what the headlines and media outlets have been telling us for a while now – that there's been a continued spike in a variety of cyber crimes. The new report also suggests that attackers are becoming more innovative, organized, and sophisticated.

The 2018 report has these key findings:

- A 600% increase in Internet of Things (IoT) attacks
- An 8,500% increase in "cryptojacking," which is the secret use of a computing device to mine cryptocurrencies
- A 200% increase in malware implants
- A 54% increase in the spread of mobile malware
- An evolution of ransomware into more varieties with lower ransom fees

The report is available on security firm Symantec's home page – *www.symantec.com.*

TRANSPARENCY

Nevada SC Says Officials' Private Devices Not Exempt

Nevada's highest court has reversed a lower court ruling by affirming that personal devices used by public officials are subject to disclosure rules under Nevada's public records law.

In a unanimous decision in March, the state's supreme court reversed a decision by Washoe County District Court Judge Steven Kosach that denied a records request for any communications made by officials on official business on their own devices.

"We conclude that the (Nevada Public Records Act) does not categorically exempt public records maintained on private devices or servers from disclosure," Judge Michael Cherry wrote in the order. "To withhold a public record from disclosure, the government entity must present, with particularity, the grounds on which a given public record is exempt."

As reported by *The Nevada Independent*, the case was first brought by a residents association against county commissioners over an industrial zoning decision. As part of the case, the association made a public records requests for all relevant communications that were made on private and public devices.

The Nevada Policy Research Institute (NPRI), a small-government think tank, praised the ruling:

"The ruling – drawing on the plain language of the law and the intent behind

it – established jurisprudence which will act as a bulwark against those who would seek to undermine Nevada's Public Records Law by choosing to conduct public business on private devices," said NPRI's Robert Fellner.

HEALTH RECORDS

Facebook Began Secret Mission to Get Patient Data from Hospitals

As widely reported in April, Facebook held conversations with hospitals and medical groups earlier this year to discuss how they could share data about their most vulnerable patients.

According to *cnbc.com*, Facebook's goal was to build profiles that included patients' medical conditions and other information that health systems maintain, and then to combine it with social and economic factors gleaned internally.

Apparently, the information shared would obscure personally identifiable data, such as the patient's name, but such anonymity would then collapse if Facebook followed through on its plans to use a computer science method called "hashing," which matches – identifies, essentially – individuals who fit into both sets.

Health policy experts said the initiative would be problematic if Facebook did not think through the privacy implications.

"Consumers wouldn't have assumed their data would be used in this way," said Aneesh Chopra, former White House chief technology officer. "If Facebook moves ahead (with its plans), I would be wary of efforts that repurpose user data without explicit consent."

Reportedly, the initiative never went past the planning phases, and Facebook has said the project is on hiatus so it can focus on "other important work, including doing a better job of protecting people's data."

"This work has not progressed past the planning phase, and we have not received, shared, or analyzed anyone's data," a Facebook spokesperson told CNBC.

OPTICAL CHARACTER RECOGNITION

Using Artificial Intelligence to Unlock the Vatican's Archives

The Vatican's secret archives are the stuff of legend, according to *TechnologyReview.com.* They fill 85 kilometers of shelving in Vatican City and contain private letters and other documents of former popes, dating to the eighth century.

Because the archives are closely guarded, scholars have had limited access to the documents. It is known that the archives contain a 60-meter scroll detailing the trials of the Knights Templar, which started in 1307; and there are letters to popes from Michelangelo, Henry VIII (requesting a marriage annulment), and Mary, Queen of Scots (begging for intercession before her beheading).

The archives also hold more recent correspondence, including letters from Abraham Lincoln and Jefferson Davis during the U.S. Civil War; and records relating to Pope Pius XII and his dealings with the Nazis during the second world war – records that have never been published. In fact, no records have been made public since 1939.

TechnologyReview.com says that publishing records is forbidden, but the Vatican is seeking to preserve many documents for further study. The quantity is so voluminous that transcribing them by hand is impractical.

The apparent solution is a technology called *machine vision*. Developed by Donatella Firmani and other scholars at Roma Tre University in Italy, the technology is expected to automatically transcribe a part of the Vatican secret archives called the *Vatican Registers*, which consists of more than 18,000 pages of official 13th century correspondence between the Catholic Church and kings, queens, and political and religious institutions across Europe.

Medieval texts present a unique challenge for optical character recognition (OCR), whose algorithms do not work well because the manuscripts are written in varying styles with different ligatures (characters that combine adjacent letters) and with idiosyncratic abbreviations. The new response is to train an OCR system to divide each word into a series of strokes that fit together like a jigsaw puzzle. The system then tries to fit them to form known letters, and it ultimately filters out those results that are not grammatical.

For example, a common pattern of strokes can be interpreted as "iii" or as "m," but the former can be ruled out as grammatically unsound. The same strokes might also represent "in" or "ni"; the system must study the word and its context more closely before deciding.

Firmani's team created a data set to train a machine-vision system based on a neural network. This data set was labeled so that the system could learn what letters were represented by different combinations of strokes.

The team also used crowdsourcing to complete this annotation. They presented the jigsaw segmentation of words as a pattern recognition problem to 120 high school students. Together, the students labeled a 15,000-character training data set in a couple of hours.

"We were able to generate the exact transcription for 65 percent of the word images of our dataset," said Firmani.

How the Vatican secret archives will use this technology isn't clear. But the tools that Firmani and his colleagues are developing should help scholars make progress toward using data-driven tools to better understand historical documents and trends.

Take Our Latest One-Minute *IM* Poll

Citing the magnitude of the project, our Business Matters sub-feature makes a case for outsourcing IM or IG program design and implementation. Please visit our latest poll at ***http://imm.explorearma.org/outsideconsulting*** to tell us for what projects your organization has engaged, is engaging, or would like to engage an outside IM or IG consultant.

Read the article that prompted this survey on page 36.

In the March/April IM poll, the percentage of survey respondents (21) who said IM collaborates with each of these functional areas is:

- Business units (100%)
- Information security (85.7%)
- Privacy (90.5%)
- IT and risk/compliance (tie at 76.2%)
- Legal (90%

Take or see results for previous polls at ***http://imm.explorearma.org/RIM_Polls.***

MS *in* COMMUNICATIONS & INFORMATION MANAGEMENT

YOUR CAREER GOALS ARE IN REACH.

- Classes start every October, February, and June
- 36 credits, offered 100% online
- Our extraordinary faculty are accomplished in the field
- Financial Aid available
- No GRE or GMAT required

ENROLLING NOW!
Classes begin June 25th

For more information visit **BAYPATH.EDU**

BAY PATH UNIVERSITY
1897
FOR A CONSTANTLY CHANGING WORLD

FEDERAL TRANSPARENCY

NARA's 'Unauthorized Destruction' Chart Suggests Troubling Trends in Retention, Transparency

Unredacted.com reports that the U.S. National Archives and Records Administration (NARA) has published its first "unauthorized disposition of federal records" chart, which tallies NARA investigations in fiscal year 2017 into the "actual, impending, or threatened unlawful removal, defacing, alteration, corruption, deletion, erasure, or other destruction of records."

The chart reveals that the departments of State, Interior, Agriculture, and Justice were probed the most often, typically for the disappearance of records and the use of encrypted messaging applications.

Unredacted lists these key findings from the NARA chart:

- The Environmental Protection Agency allegedly used an encryption messaging application called Signal to circumvent the government's ability to monitor communications related to government business and to covertly avoid federal records requirements.
- The National Oceanic and Atmospheric Administration allegedly destroyed electronic messages through Skype and Google Chat that concerned discussions of new regulations in the fishing industry.
- The Department of Defense allegedly destroyed documents in an internal investigation of a former National Security Agency whistleblower.

The chart, which is updated monthly, is available at *www.archives.gov/records-mgmt/resources.*

FREEDOM OF INFORMATION

City Seeks to Restrict Hours Spent on Information Requests

Amarillo.com reports that the City of Amarillo, Texas, has taken steps toward establishing monthly and yearly limits on time that city personnel can spend on information requests without recovering costs attributable to that personnel time. The city council voted 4-1 to approve the first reading of Ordinance 7717.

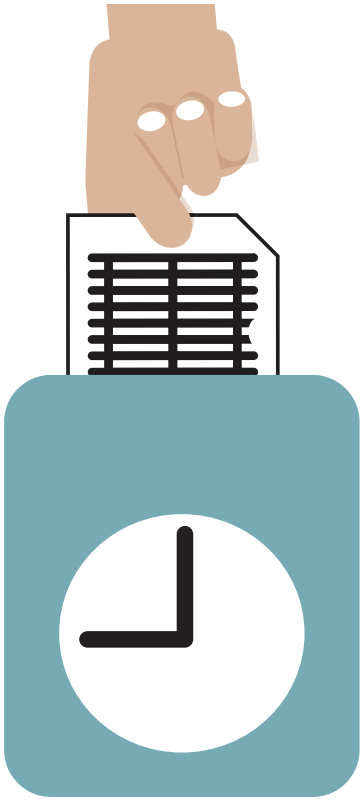
Earlier, the state had revised the Public Information Act to allow governmental entities to establish such limits. According to *Amarillo.com*, city officials wished to mirror the state's action.

"We are recommending you adopt the change to our code of ordinances related to the number of hours a single requester can cause city personnel to research their Public Information Request without paying for that service," City Attorney Mick McKamie said in addressing the city council regarding the proposed modification. "The statute allows us to keep a record of the number of hours a single requestor causes the labor of city personnel to be used to respond to the request and after they reach 36 hours a year or 15 hours any particular month, the city secretary would put them on notice that they would be responsible for those labor charges."

He said personnel in all city departments allocate thousands of hours yearly responding to Public Information Act requests – noting they are happy to do so.

The lone dissenting vote was cast by Elaine Hays, who later expressed reservations about the approval. "This could become a financial restriction for some individuals who are making requests and that is a concern," she said.

The ordinance says the city secretary or a designee would be responsible for maintaining records of the cumulative amount of personnel time spent complying with requests for public information from each individual requestor.



TRANSPARENCY

Report Says Canadian Government Should Reform its Access to Information Act

An independent report on Canada's transparency efforts says the government should make "robust reforms" to the Access to Information Act. According to *TheGlobeandMail.com,* the report, released in mid-April, calls for funding of federal openness commitments, better response to advice from interested parties, and increased cooperation with First Nations on issues of transparency.

The report was included in the Open Government Partnership's evaluation scheme, which judges the progress of each of the global partnership's 75 member governments, including Canada.

The partnership selected Michael Karanicolas, president of the Right to Know Coalition of Nova Scotia, to conduct the assessment of Canada. Karanicolas met with officials from 16 governmental agencies and departments.

"There is no question that the landscape for open government in Canada has improved dramatically since the last election," Karanicolas said. "However, now that the low-hanging fruit has been plucked, Canada is at a crossroads. There is potential for Canada to establish itself as a global open government leader, but this will require bold and ambitious proposals, rather than more incremental steps forward."

In previous actions, Canada had committed to increasing digital access to museum collections and scientific data and to enhancing transparency on government spending.

Last June, the Trudeau government introduced legislation that would give the information commissioner new authority to order the release of files and to make routine the release of briefing notes and expense reports. The information commissioner's office and some civil society groups say the proposals were too timid.

"Access to information is a central pillar of open government, such that Canada's lack of progress on this critical indicator is beginning to overshadow the excellent work being done elsewhere," Karanicolas' report says.

What needs to be done, according to the report, is expand the right to file access requests to the office of cabinet and prime minister; create a duty for officials to write things down; introduce binding timelines for responding to requests; and narrow the broad exceptions that now permit agencies to withhold information.

PRIVACY

Queensland Bans Ministers from Using Private E-mail and Messaging

Annastacia Palaszczuk, the Queensland premier, has banned her ministers from using private e-mails and encrypted messaging services to discuss official business.

As reported on *TheGuardian.com*, the new guidelines come in response to a controversy involving Minister Mark Bailey's use of a private e-mail account.

It was expected that Premier Palaszczuk would ban the use of private e-mails, but the new guidelines go further; they also ban the use of Facebook messenger, SnapChat, and encryption services Wickr and WhatsApp. (Prime Minister Malcolm Turnbull has admitted to using Wickr and WhatsApp to communicate with official colleagues and the media.)

Last summer, the Crime and Corruption Commission found "a reasonable suspicion of corrupt conduct" for Minister Bailey having potentially destroyed public records.

Queensland's opposition leader has repeatedly called for Bailey to resign over his use of the private e-mail account, but an investigation by the state archivist ultimately found "no evidence" to suggest Bailey wanted to "conceal corrupt conduct," and he was reinstated ahead of the November 2017 election.

PERMANENT DESTUCTION

Data Must be Properly Removed When a Business Closes

A company as large as Toys 'R' Us would likely have countless desktop computers, laptops, servers, external drives, printers, scanners, tablets, and so forth, all containing corporate, customer, and employee data that might date back to dozens of years.

What happens to those devices and all of that data when a company shuts its door for the final time? In the case of Toys 'R' Us, those are a lot of doors: 735 stores in the United States alone.

In a recent article, *SecurityBoulevard.com* raises this very question.

The concern, of course, is that unmeasured bytes of data could become vulnerable to loss or theft.

"Unfortunately, dragging files to the 'Recycle Bin' on computers and emptying that bin or reformatting drives before dumping them into the dumpster, recycling them or even reselling them, could turn into a privacy nightmare," writes Russ Ernst of *Security Boulevard*.

And that's not to mention the major regulatory violations and legal fines that could be incurred from improper handling of all of that data.

Reporter Ernst states that retailers such as Toys 'R' Us have a corporate responsibility to ensure that all data is expunged permanently from IT assets so it won't fall into the wrong hands. He writes: "Leaking corporate or customer data, whether it's accidentally or intentionally, can have major financial, legal and reputational ramifications – going far beyond the standard implications of shuttering a business."

To properly mitigate the risks of data exposure, all companies, no matter their operating status, must follow the necessary data retention and data removal policies throughout the data life cycle – and be especially cognizant of the "end of life" stage when employees leave.

Ernst reminds us that the recycle bin mechanism is not enough: data is not permanently deleted when it tumbles into the electronic can. Likewise, other common attempts at deleting data, such as removing programs or re-installing software, do not permanently remove information either: such tactics just move it from one location to another. That is why companies that dissolve often have millions of files that are easily accessible to those who know the tricks.

"The right way to permanently erase files from computers/laptops, servers and external drives is to overwrite the data with zeros and ones multiple times," he advises.

Further, to make sure deleted information cannot be recovered, such organizations must use certified tools that securely erase data and comply with such regulatory standards as the Health Insurance Portability and Accountability Act, Sarbanes-Oxley, and others. These proper tools can also provide evidence that the data has been completely and permanently removed.

Ernst concludes with this admonition: "For those businesses that overlook permanently erasing critical information stored across IT assets and storage environments, it will be as if they've sent hundreds of files directly into a criminal's Recycle Bin, making them easily retrievable and susceptible to a data breach."

FEDERAL POLICY

Oversight Panel Advances Legislation on Records Preservation, Transparency

In March, the House Oversight and Government Reform Committee approved several bills aimed at preserving electronic records, improving the customer experience, and posting more information online, according to *FCW.com*.

The Electronic Message Preservation Act, which had been introduced by Elijah Cummings (D-Md.) in 2013, 2015, and 2017, made it out of committee for the first time. The bill would empower the national archivist to issue rules requiring federal agencies to capture and preserve digitally created records and require those records to be "readily accessible" through electronic searches.

The committee also advanced a bill that would make sure agencies make available records covered by the Freedom of Information Act to NARA's Office of Government Information Services (OGIS) upon request. OGIS is the Justice Department entity that generates governmentwide FOIA policy.

Critical Efficiency Improvements

EXL improved mail- and document-handling operations for a key client using OPEX Corporation's Universal Document Scanning Workstations.

When it comes to document management, productivity and accuracy are critical and require enterprise-class technology to ensure efficiency and traceability. EXL was able to improve efficiency by several hours per day and reduce resource requirements significantly using OPEX® FalconRED® and Falcon® document scanners for a high-volume customer.

EXL is a global operations management and analytics company based in New York. As part of its service offerings, the company provides mailroom and document services to companies primarily in the finance, accounting, and insurance markets.

The company operates customer mail centers both on-site and in its own facilities where document imaging and document management are key activities. "Our imaging center really feeds the process for the folks doing the work at these companies," says Glen Baker, Vice President of Life and Annuities at EXL. "Images are our lifeblood."

At one particular customer site, however, the quality and reliability of those images were in question. The company operated a mailroom for the customer where staff received, prepped, and scanned documents on a conventional production class scanner. The facility processes between 6,000 and 6,500 documents per day, with each document containing 3.5 to 4 pages. "The preparation process caused some problems in terms of quality and productivity," Baker says. "We went back and revisited that entire environment with an eye toward swapping out the software and hardware."

Working closely with the client, EXL created a scorecard and wrote a detailed requirements document that was used to evaluate the new scanning hardware. "We wanted something that was production-quality and could help take us from receipt through archiving," Baker says.

Eventually, EXL narrowed their choices down to the OPEX Falcon and FalconRED series of document scanning workstations and another scanner manufacturer. OPEX ultimately won out, in part because of the way the scanners handled the archiving process. "We would have the ability to tag information when it comes through and follow those documents throughout the entire process for traceability," Baker says. "It also required less customization out of the box." The second important feature of the Falcon series was OPEX's one-touch prep and scan environment.

EXL also replaced the existing software implementation with Hyland Software's OnBase® product. "We had used OnBase for many years at our own New Jersey scan center," Baker says. "When we re-evaluated the client facility, we found we could get almost 95 percent of the features we needed out of the box with OnBase as opposed to the previous software."

Minimize Labor, Maximize Quality

EXL has deployed five FalconRED scanners and one Falcon scanner at the site. FalconRED combines the Falcon scanner with the OPEX Model 72 Rapid Extraction desk. This unrivaled combination of envelope opening, content extraction, and document imaging makes FalconRED the most efficient, secure, and cost effective way to scan directly from sealed envelopes with no added prep operators needed.

Because the customer had multiple lines of business operating out of the same mailroom, EXL was able to install the new solution in phases. Initially, they brought in a demo Falcon unit for evaluation. "After that, we took the big leap," Baker says. "We were convinced this was the answer we would need going forward. We went through the process of getting the software up and running while the machines were being built and had a parallel document processing operation in place [using both new and old equipment] as we went through each phase."

Read the entire article here.

For more information visit www.opex.com

OPEX® CORPORATION

SOCIAL MEDIA

Texas Town Opts for Software to Archive Social Media Posts

Before Archive Social, we were taking pictures of posts on our pages and saving them as JPEGs and putting them in a file."

That's how the town of Dripping Springs, Texas, formerly captured the social media posts on its own media, according to Andrea Cunningham, city secretary. But in April the town purchased Archive Social, a software that automates the process of archiving those records, even if such posts have been deleted.

As reported on *HaysFreePress.com*, the purchase will help Dripping Springs monitor its six Facebook pages and two Twitter accounts. As a result, Dripping Springs can archive the posts for the purposes of transparency and to track any citizen comments or concerns.

"This year alone we have had around four people ask, through an open records request, for social media posts on the city's pages," Cunningham told *Hays Free Press*. "This allows us to archive that information and stay on top of our duty to be transparent for our citizens."

Texas law requires cities to provide its citizens access to public records and information, including physical and digital copies of any legislation, meetings, citizen comments, development plans, and other city records.

Archive Social already works with two of the biggest cities in the state. In Austin, the software helps the police department manage social media to see where the risks are happening in real time. In Dallas, the city employs the software to make most of its data available through "Dallas Data Points," a dashboard that provides visibility into the city's progress in such areas as public safety, economic vibrancy, e-government, and more.

Cunningham said the city will not release private information such as addresses, medical information, or names. Further, social media pages not owned by the city, such as community forums, will not be subject to this new program.

The subscription to Archive Social will cost $200 a month.

FEDERAL RECORDS

NARA Publishes Guidance on Managing Permanent E-Records

According to the official blog of the Office of the Chief Records Officer, the National Archives has published new guidance on managing electronic records. *Criteria for Successfully Managing Permanent Electronic Records* is designed to support the Managing Government Records Directive (M-12-18), which states "By December 31, 2019, all permanent electronic records in Federal agencies will be managed electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format."

According to the blog, the guidance describes what agencies should consider from a high level when managing their permanent electronic records. It includes operational activities, which describe practical "how to" instructions for accomplishing key tasks agencies must carry out as they move towards the 2019 target of managing all permanent electronic records in electronic format. The guidance also reinforces the value of NARA's Universal Electronic Records Management (ERM) Requirements.

The publication can be accessed here: *www.archives.gov/files/records-mgmt/policy/2019-perm-electronic-records-success-criteria.pdf.*

NATIONAL ARCHIVES

BLOCKCHAIN

Samsung Is Set to Embrace Blockchain for its Supply Chain

According to *Bloomberg.com,* Samsung, the world's largest maker of smartphones and semiconductors, is considering using blockchain technology to manage its vast global supply network.

The announcement was made by Song Kwang-woo, the blockchain chief at Samsung SDS Co., which handles the company's logistics, technologies, and information. The system could trim shipping costs by 20%, according to Song.

Samsung is one of the first global manufacturers to seriously consider using the distributed ledgers in its operations. SDS is focusing on using the system for Samsung Electronics, the conglomerate's crown jewel.

"It will have an enormous impact on the supply chains of manufacturing industries," said Song. "Blockchain is a core platform to fuel our digital transformation."

Bloomberg says that blockchain technology is touted as a breakthrough that will transform the way transactions are recorded, verified, and shared. Gartner Inc. predicts blockchain-related businesses will create $176 billion of value by 2025.

In the shipping industry, those who support blockchain claim it reduces the time needed to send paperwork back and forth and to coordinate with port authorities.

A blockchain system could help Samsung cut the time lag between product launches and their shipments, making it simpler to respond to rival products and shifting consumer appetites in emerging markets like China, says Cheong Tae-su, a professor at Korea University in Seoul.

"It cuts overhead and eliminates bottlenecks," Cheong told *Bloomberg*. "It's about maximizing supply efficiency and visibility, which translates into greater consumer confidence."

PRIVACY

U.S. Commerce Department Updates Actions to Support the Privacy Shield

The U.S. Department of Commerce recently posted an update on steps it has taken to support commercial and national security issues relating to the Privacy Shield frameworks, reports *Hunton-PrivacyBlog.com.*

Relative to commercial enhancements, Commerce has ensured an enhanced certification process through such steps as implementing more rigorous company reviews and reducing opportunities for false claims; increasing the monitoring of companies' compliance; performing random spot checks for certified organizations; conducting proactive checks for false claims online; and confirming a list of arbitrators to ensure that EU individuals have recourse to arbitration.

Regarding national security, Commerce has confirmed that Presidential Policy Directive 28 (as regards the collection and use of "signals intelligence") remains in place without amendment; that the intelligence community reaffirms its commitment to civil liberties, privacy, and transparency through the updating of Intelligence Community Directive 107; that independent oversight will be achieved through the nomination of three people to the Privacy and Civil Liberties Oversight Board, thus restoring the agency to quorum status; that individual redress through the creation of a ombudsperson will be made available; and more.

CYBERCRIME

Big Tech Companies Are Forming Alliance to Fight Cyber Attacks

Some prominent members of the technology industry are uniting in an effort to combat the epidemic of cyber attacks. Reporter Jon Fingas of *Engadget.com* says 34 companies have signed the Cybersecurity Tech Accord, agreeing to defend customers globally from any and all hacks. The pact includes promises to boost defenses, establish more partnerships to share threats and vulnerabilities, and refuse to help governments launch cyberattacks.

Among the more familiar names in the accord are Cisco, Dell, Facebook, HP, Microsoft, and security firms Avast, FireEye, and Symantec. Other companies that are "trusted" and share "high cybersecurity standards" are welcome to join the accord, according to Fingas.

While the accord sets out to present a united front in which companies work together, Engadget's Fingas notes the pact lacks specific action points at this stage: "it's easy to make general statements of principle, it's another to back those up."

Fingas also draws attention to notable omissions in the lineup, such as Apple, Amazon, and Twitter. He concludes that the accord is an important start to fending off cyberattacks, but it may need to expand significantly beyond its existing member list to be truly effective.

BIOMETRICS

Class Action Suit Over Facebook's Facial Recognition Will Proceed, Says Fed Judge

According to *Engadget.com*, Facebook has for years tried to squelch a lawsuit that claims the company's facial recognition technology violates Biometric Information Privacy Act (BIPA), an Illinois law that prohibits the collection of biometric data. In April, a federal judge in San Francisco, James Donato, gave the case the go-ahead to proceed as a class-action suit.

Facebook claimed the law was not applicable because its servers are not located in Illinois, but Judge Donato held that the location isn't "a dispositive factor."

Engadget reports that the class action will consist of users in the state "for whom Facebook created and stored a face template after June 7, 2011," which was the date the company rolled out "Tag Suggestions," a way to recognize and tag people in photos.

(For more information on biometric identifiers and BIPA, see this issue's feature article, "Understanding Biometrics' Obligations," which begins on page 20.)