UNITED STATES - THE CLOUD ACT HAS BEEN PASSED

A long-running court battle between Microsoft and the US government about whether the latter had the right to access emails held in Microsoft’s Irish data centre has come to an end after a judge dismissed the case, ruling it to be "moot" due to the recent passing of the Cloud (Clarifying Lawful Overseas Use of Data) Act.

Prior to the enactment of the CLOUD Act, the Supreme Court was poised to rule in the case *Microsoft Corporation v. United States of America*, No. 17-2, on whether the 1986 Stored Communications Act (SCA) permitted the use of a warrant to obtain electronic communications stored by a U.S. company on foreign servers.

The Clarifying Lawful Overseas Use of Data (Cloud) Act, which was passed as part of the recent omnibus spending bill, is designed to help find solutions to the challenges of cross-border data collection by foreign governments and law enforcement. It updates the SCA, giving executive branch agencies the ability to enter into “executive agreements” with foreign governments (if they meet a detailed list of requirements) to facilitate cross-border access to data for criminal investigations.

In addition, the CLOUD Act provides that a provider of electronic communication service or remote computing service must comply with the requirements of the SCA to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, “regardless of whether such communication, record, or other information is located within or outside of the United States.”.

In a blog post, Microsoft President Brad Stone wrote: “*The proposed CLOUD Act creates a modern legal framework for how law enforcement agencies can access data across borders. It’s a strong statute and a good compromise that reflects recent bipartisan support in both chambers of Congress, as well as support from the Department of Justice, the White*
House, the National Association of Attorneys General and a broad cross section of technology companies. It also responds directly to the needs of foreign governments frustrated about their inability to investigate crimes in their own countries. The CLOUD Act addresses all of this, while ensuring appropriate protections for privacy and human rights. And it gives tech companies like Microsoft the ability to stand up for the privacy rights of our customers around the world. The bill also includes a strong statement about the importance of preventing governments from using the new law to require that U.S. companies create backdoors around encryption, an important additional privacy safeguard.”

Read more:

Everything You Need to Know About the CLOUD Act

UNITED STATES – ALL 50 STATES IN THE US NOW HAVE A DATA BREACH NOTIFICATION LAW

Alabama Republican Gov. Kay Ivey has signed a bill that makes her state the 50th and final one to enact a data breach notification law.

The law requires organizations and agencies to notify data breach victims within 45 days after a breach has been discovered if it is reasonably likely to cause substantial harm, becoming the last US state to enact such a statute. The notification could be delayed if it would interfere with a law enforcement investigation.

The law, which takes effect May 1, includes medical and health insurance information in the definition of “personally identifying information” subject to notification.

Under the law, the Attorney General can fine violators up to $5,000 per day and file lawsuits on behalf of the breach victims.

“Alabama consumers finally join the rest of America in having the right to know if their personal information is stolen or compromised in a data breach,” said state Attorney General Steve Marshall.

Until recently, Alabama and South Dakota were the only U.S. states that did not have data breach notification laws in place.

On March 21 of this year, South Dakota Governor Dennis Daugaard signed that state’s first data breach notification law, which takes effect July 1. That law requires organizations and agencies to information data breach victims within 60 days of breach discovery or notification by a third party.

Read more:

Alabama Last US State to Enact Data Breach Notification Law

UNITED STATES - RECENT DATA BREACHES MAKING HEADLINES

Adding to the long list of recent announcements of data breaches, travel booking website Orbitz, a subsidiary of the American travel company Expedia which owns about 200 travel booking websites in about 75 countries, announced that on March 1, 2018 it discovered a potential data breach that exposed the personal information of thousands of customers. The breach may have exposed information tied to about 880,000 credit cards.
The consumer data which is the subject of the breach is from an older booking platform where information may have been accessed between October and December 2017. Orbitz partner platform data, such as travel booked via Amex Travel, submitted between January 1, 2016 and December 22, 2017 may also have been compromised. The company has stated that customer names, payment card information, dates of birth, email addresses, physical billing addresses, gender, and phone numbers may have been accessed, but Orbitz cannot confirm with “direct evidence” that any information was taken from the website.

Orbitz has stated that it began working with a forensic investigation firm, cybersecurity experts, and law enforcement once the breach was discovered in order to “eliminate and prevent unauthorized access to the platform.” The company says its current site, Orbitz.com, wasn’t affected. Orbitz is notifying customers who may have been impacted and is offering a year of free credit monitoring.

More recently, Panera Bread joined the list of companies hit by a data breach, acknowledging that customer information was vulnerable on its company website for at least eight months. The records belonged to customers who had registered for the MyPanera program to order food online. The details exposed included their names, email and physical addresses, birthdays, and the last four digits of user credit card numbers, according to the security news site Krebs on Security. Customers’ Panera loyalty card numbers were also exposed, according to Krebs on Security, which estimated that about 37 million customers had been affected by the leak, though experts say the true number of compromised records may never be fully known.

Likewise, Under Armour announced that data from some 150 million MyFitnessPal diet and fitness app accounts was compromised in February, in one of the biggest hacks in history. The stolen data includes account user names, email addresses and scrambled passwords for the popular MyFitnessPal mobile app and website, Under Armour said in a statement. Social Security numbers, driver license numbers and payment card data were not compromised, it said. It is the largest data breach this year and one of the top five to date, based on the number of records compromised, according to Security Scorecard. Nevertheless, the company has received praise from security professionals for its response to the data breach. “Praising a company after a breach is difficult, but we should give UnderArmour credit for keeping payment information separate from profile information,” said James Lerud, head of Verodin’s Behavioral Research Team. “They appear to be handling this incident in a responsible way by notifying the public and requiring password resets.” Forrester Security Expert Jeff Pollard said that while the breach affected a large number of accounts, "Under Armour is showing it learned some lessons from companies breached in recent months by notifying its customers rapidly after discovering the intrusion."

Meanwhile, there were reports that Boeing has been hit by the same WannaCry computer virus that struck thousands of computer systems in more than 70 countries around the world last year. The New York Times reports that, in an internal memo, Mike VanderWel, chief engineer of Boeing Commercial Airplane production engineering, said the attack was “metastasizing” and he worried it could spread to Boeing’s production systems and airline software. “We are on a call with just about every VP in Boeing,” Mr. VanderWel wrote. The memo called for “all hands on deck.” In addition, the City of Atlanta was hit with a different ransomware (known as SamSam) and is still reeling from the fallout.

Last but not least, department store chain Sears Holding Corp and Delta Air Lines Inc said on Wednesday 4th April that some of their customer payment information may have been exposed in a cybersecurity breach at software service provider [24]7.ai. Sears said it was notified of the incident in mid-March and the incident led to unauthorized access to the credit card information of under 100,000 of its customers.
Technology firm [24]7.ai, which provides online support services for Delta, Sears and Kmart among other companies, found that a cybersecurity incident affected online customer payment information of its clients, it said.

Read more:

Orbitz says a possible data breach has affected 880,000 credit cards

Panerabread.com Leaks Millions of Customer Records

Under Armour says 150 million MyFitnessPal accounts breached

Under Armour deftly manages breach, dodges GDPR scrutiny

Boeing Possibly Hit by ‘WannaCry’ Malware Attack

Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand

Sears Holding, Delta Air hit by customer data breach at tech firm

GLOBAL - FACEBOOK SCANDAL, A ‘GAME CHANGER’ IN DATA PRIVACY REGULATION?

According to Bloomberg, revelations that data belonging to as many 87 million Facebook Inc. users and their friends may have been misused became a game changer in the world of data protection as regulators are looking to raise awareness about how to protect information.

The report states that Elizabeth Denham, the U.K. privacy regulator leading the European investigations into how user data ended up in the hands of consulting firm Cambridge Analytica, will say in a speech that the technology industry and regulators must improve the public’s trust and confidence in how their private information is handled.

“The dramatic revelations of the last few weeks can be seen as a game changer in data protection,” Denham, the U.K. Information Commissioner, will say at her agency’s annual conference for data-protection practitioners. “Suddenly, everyone is paying attention.”

Likewise, Apple’s Chief Executive Tim Cook has called for stronger privacy regulations that prevent the misuse of data in the light of the controversial leak of Facebook user information. Cook called for “well-crafted” regulations that prevent the information of users being put together and applied in new ways without their knowledge during a session on global inequality at the annual China Development Forum in Beijing.

“I think that this certain situation is so dire and has become so large that probably some well-crafted regulation is necessary,” Cook said after being asked if the use of data should be restricted in light of the Facebook incident.

“The ability of anyone to know what you’ve been browsing about for years, who your contacts are, who their contacts are, things you like and dislike and every intimate detail of your life -- from my own point of view it shouldn’t exist.”
Read more:

Facebook Scandal a ‘Game Changer’ in Data Privacy Regulation

Apple’s Tim Cook Calls for More Regulations on Data Privacy

UNITED STATES - SANCTIONS FOR INTERFERENCE WITH 2016 ELECTIONS AND MALICIOUS CYBER ATTACKS

On March 15, 2018, the U.S. Department of the Treasury’s announced that its Office of Foreign Assets Control (OFAC) designated five entities and 19 individuals under the Countering America’s Adversaries Through Sanctions Act (CAATSA) as well as Executive Order (E.O.) 13694, “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,” as amended, and codified pursuant to CAATSA.

Treasury Secretary Steven T. Mnuchin stated that “The Administration is confronting and countering malign Russian cyber activity, including their attempted interference in U.S. elections, destructive cyber-attacks, and intrusions targeting critical infrastructure...These targeted sanctions are a part of a broader effort to address the ongoing nefarious attacks emanating from Russia. Treasury intends to impose additional CAATSA sanctions, informed by our intelligence community, to hold Russian government officials and oligarchs accountable for their destabilizing activities by severing their access to the U.S. financial system.”

The government's action is an attempt to counter what it considers to be Russia’s continuing destabilizing activities, ranging from interference in the 2016 U.S. election to conducting destructive cyber-attacks, including the NotPetya attack, a cyber-attack attributed to the Russian military on February 15, 2018. The NotPetya cyber-attack has been called the most destructive and costly cyber-attack in history and resulted in billions of dollars in damage across Europe, Asia, and the United States, and significantly disrupted global shipping, trade, and the production of medicines. In addition, several hospitals in the United States were unable to create electronic records for more than a week. The government also stated that at least as early as of March 2016, the Russian government cyber actors have targeted U.S. government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.

As a result of the government's action, all property and interests in property of the designated persons subject to U.S. jurisdiction have been blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

Read more:

Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks

UNITED STATES - YAHOO TO SETTLE DATA BREACH CLASS ACTION SUIT FOR $80M USD

Yahoo has agreed to pay $80m USD to settle a class action suit filed by investors relating to data breaches affecting three billion customers.
Shareholders filed the suit in January 2017 alleging that the web service provider violated federal securities law fraud by failing to promptly disclose the breaches which caused a subsequent stock price dive.

If approved by the court, this settlement will be the first of its kind and experts are divided over whether it will spark more federal securities lawsuits following major breaches.

Yahoo revealed the full extent of the 2013 security incident which led to the breach of three million customer records, in October 2017 and disclosed an incident that occurred 2014 in September of 2016 which is thought to be the work of state-sponsored hackers and resulted in a breach of 500 million accounts.

Read more:

Stipulation and Agreement of Settlement

SINGAPORE - NEW MEMBER OF THE APEC DATA PRIVACY SYSTEM

Singapore has become the latest member of the APEC Cross-Border Privacy Rules, recognizing that Singapore’s personal data protection law is aligned with the system to facilitate data flows between economies and prevent accidental disclosure and misuse of personal data derived from transactions online.

Singapore is the APEC Cross-Border Privacy Rules System’s sixth participant, joining Canada, Japan, Korea, Mexico and the United States.

“The seamless exchange of personal data will enable certified Singapore businesses to plug into even more regional and global business opportunities. Meanwhile, our consumers will enjoy greater peace of mind when they shop or use vital services online,” said Tan Kiat How, Singapore’s Infocomm Media Development Authority CEO and Personal Data Protection Commissioner. “Our entry into the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems will benefit Singapore’s businesses and consumers,” Tan continued.

Under the APEC Cross-Border Privacy Rules System, the privacy policies and practices of companies operating in Singapore, like those in other participating APEC economies, will voluntarily follow a set of commonly agreed rules based on the APEC Privacy Framework. Such companies are assessed and certified by a third-party verifier known as an Accountability Agent.

“The growth of the APEC Cross-Border Privacy Rules System reflects the increasing need for interoperability between differing privacy regimes, reducing barriers to digitally-based trade between them and promoting greater trust and entrepreneurship online,” explained Shannon Coe, Chair of the APEC Electronic Commerce Steering Group, which administers the initiative.

“As big data, artificial intelligence and other innovations translate into new business ventures, the need for seamless and secure data flows will only increase in importance,” concluded Coe. “The inclusion of Singapore in the APEC Cross-Border Privacy Rules System is another step in the right direction and builds momentum for its continued development.”

Read more:

Singapore Joins APEC Data Privacy System
GERMANY - RIGHT TO BE FORGOTTEN RULING

The German Federal Court of Justice ruled in February that Google is not obligated to ensure that websites are free from defamatory content before displaying links to them in search results.

The plaintiffs, two individuals, sought to prevent Google's search engine from displaying links to websites on which the plaintiffs were verbally attacked by other internet users, to set up search filters to keep those websites from appearing in future search results, to provide information about the users who had posted the offending comments and payment of damages alleging that Google was, in part, liable for the violation of their rights and had a duty to screen and not to display the defamatory material to others online.

The case comes in the context of debate about the so-called “right to be forgotten.”

The Federal Court of Justice ruled that a search engine operator need only take action if it is notified of a clearly recognizable violation of individuals’ rights, rather than checking ahead of time whether the content complies with the rules. The court stated that “Instituting a general duty to inspect the content would seriously call into question the business model of search engines, which is approved by lawmakers and wanted by society" and "Without the help of such search engines it would be impossible for individuals to get meaningful use out of the internet due to the unmanageable flood of data it contains.”

In May 2014, the Court of Justice of the European Union (ECJ) ruled that people could ask search engines, such as Google and Microsoft’s Bing, to remove inadequate or irrelevant information from web results appearing under searches for people’s names - dubbed the “right to be forgotten”. According to Google's transparency report, since 2014 Google has since received requests for the removal of more than 2.4 million website links and accepted about 43 percent of them.

Read more:

German court: Google has no ‘duty to inspect’ websites for illegal content before displaying

AUSTRALIA - PRUDENTIAL REGULATION AUTHORITY (APRA) PROPOSES CROSS-INDUSTRY FRAMEWORK FOR THE MANAGEMENT OF INFORMATION SECURITY

The Australian Prudential Regulation Authority (APRA) has responded to the growing threat of cyber-attacks by proposing its first prudential standard on information security. APRA released a package of measures, titled Information Security Management: A new cross-industry prudential standard, for industry consultation. The package is aimed at shoring up the ability of APRA-regulated entities to repel cyber adversaries or respond swiftly and effectively in the event of a breach.

The proposed new standard, CPS 234, would require regulated entities to:

- clearly define the information security-related roles and responsibilities of the board, senior management, governing bodies and individuals;
- maintain information security capability commensurate with the size and extent of threats to information assets, and which enables the continued sound operation of the entity;
- implement information security controls to protect its information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls;
- have robust mechanisms in place to detect and respond to information security incidents in a timely manner; and
- notify APRA of material information security incidents.

Executive Board Member Geoff Summerhayes said the draft standard built on prudential guidance first released by APRA in 2010 and backed it with the force of law. "Australian financial institutions are among the top targets of cyber criminals seeking money or customer data, and the threat is accelerating," Mr Summerhayes said. "No APRA-regulated entity has experienced a material loss due to a cyber incident, but a significant breach is probably inevitable. In a worst-case scenario, a cyber-attack could even force a company out of business."

Key areas where APRA is hoping to lift standards include assurance over the cyber capabilities of third parties such as service providers and enhancing entities’ ability to respond to and recover from cyber incidents. "Cyber security is generally well-handled across the financial sector, but with criminals constantly refining and expanding their tools and capabilities, complacency is not an option," Mr Summerhayes said. "Implementing legally binding minimum standards on information security is aimed at increasing the safety of the data Australians entrust to their financial institutions and enhance overall system stability."

Read more:

Consultation on information security requirements for all APRA-regulated entities - March 2018

UNITED STATES - FTC SEEKS COMMENT ON PROPOSED MODIFICATIONS TO VIDEO GAME INDUSTRY SELF-REGULATORY PROGRAM UNDER THE COPPA SAFE HARBOR PROGRAM

The Federal Trade Commission is seeking public comment on proposals to modify a video game industry self-regulatory program that the FTC approved in 2001 under the agency’s Children’s Online Privacy Protection Rule.

The changes are being sought by the Entertainment Software Ratings Board (ESRB) and would modify the organization’s COPPA safe harbor program, which is aimed at ensuring compliance with FTC regulations and guidance related to the Children’s Online Privacy Protection Act (COPPA).

The FTC’s COPPA Rule requires, among other things, that operators of commercial websites and online services directed to children under the age of 13, or general audience websites and online services that knowingly collect personal information from children under 13, must post comprehensive privacy policies on their sites, notify parents about their information practices, and obtain parental consent before collecting, using, or disclosing any personal information from children under the age of 13.

The FTC’s COPPA Rule includes a “safe harbor” provision designed to encourage increased industry self-regulation in this area. Under this provision, industry groups and others may ask the Commission to approve self-regulatory guidelines that implement the protections of the Rule. Companies that comply with the FTC-approved guidelines receive safe harbor from agency enforcement action under the Rule.

In a notice to be published in the Federal Register shortly, the FTC is seeking comment on modifications proposed by ESRB to its COPPA safe harbor program. Among the proposed modifications, ESRB seeks to amend the definition of “personal information and data” to track the additional COPPA Rule guidance the FTC released in October 2017 related to audio recordings. Other proposed modifications include the elimination of a requirement
that new participants in ESRB’s safe harbor program complete an initial self-assessment questionnaire before joining.

Those seeking to comment should follow the directions in the Federal Register notice and will have 30 days to comment until May 9, 2018.

Read more:

[FTC Seeks Comment on Proposed Modifications to Video Game Industry Self-Regulatory Program Approved under the COPPA Safe Harbor Program](#)

**UPCOMING EVENTS**

**Internet of Things National Institute**

Format: In-Person  
Location: Crowell & Moring LLP  
Date: May 9-10, 2018  
Credits: 13.25 General CLE Credit Hours, 1.00 Ethics/Professionalism CLE Credit Hours

The Internet of Things (IOT) is defined as billions of vehicles, buildings, process control devices, wearables, medical devices, drones, consumer/business products, mobile phones, tablets, and other “smart” objects that are wirelessly connecting to and communicating with each other. This new top law practice area is raising unprecedented legal and liability issues.

As one of the most transformative and fast-paced technology developments in recent years, IoT will require businesses, policymakers, and lawyers (M&A, IP, competition, litigation, health law, IT/outsourcing, and privacy/cybersecurity) to identify and address the escalating legal risks of doing business in a connected world.

Attend this institute to:

- Discover why corporate, law firm, government, university, and other attendees gave the last two IoT Institutes rave reviews, calling it “magical,” “eye-opening,” with “rock star” speakers, and overall “a grand slam.”
- Gain insights and practical guidance on the latest legal, legislative, regulatory, and liability issues of the IoT transformation—a game-changer for businesses, policymakers, and lawyers that’s generating hundreds of billions of dollars in spending globally.
- Explore need-to-know IoT hot topics: big data/privacy, cybersecurity, litigation/mitigation, cloud/artificial intelligence, connected healthcare, ethics, global IoT product development and sales, insurance risk allocation, and homeland/national security.
- Get great value: Two (2) days of CLE credit (including ethics), including three (3) keynotes packed with compelling perspectives. There will also be opportunities for networking.
EDITORS

Paul Lanois - Mr Lanois is a global privacy, data protection and information security professional and is an attorney admitted to the Bars of the District of Columbia (DC-USA), New York (NY-USA) and the Supreme Court of the United States (SCOTUS). He regularly publishes articles on technology law and is frequently invited to speak on such topics. He has spoken at conferences across Europe, Asia and the United States. He was named a "Cybersecurity & Data Privacy Trailblazer" by the National Law Journal and an "Innovative Corporate Counsel" by Law 360. He was also recognized as a leading lawyer in The Legal 500’s GC Powerlist. He has been recognized as a Fellow of Information Privacy (FIP) by the International Association of Privacy Professionals (IAPP) and is a Certified Information Privacy Professional, with concentrations in Asian law (CIPP/A), US law (CIPP/US), European law (CIPP/E) and Canadian law (CIPP/C).

Nathan M. Barotz - Mr. Barotz has been in the private practice of law for over 25 years. A graduate of Duke University (cum laude) and the George Washington University Law School, Mr. Barotz originally developed a focus on health care law which in the last ten years has led to his strong interest the rapidly developing body of law governing IoT, cybersecurity and privacy. For the last five years, Mr. Barotz has served in the role of general counsel and compliance and privacy officer for companies utilizing telemedicine technology in post-acute patient treatment and currently serves in that role for HomeSleep, LLC, a company which specializes in diagnostic testing for sleep apnea. Mr. Barotz is a member of the New York State and Connecticut State Bars, the United States District Court Bars, Southern District and Eastern District of New York and has received his CIPP/US certification from the International Association of Privacy Professionals.

Tamara Lev - Ms. Lev is a Data Privacy attorney, specializing in: data security, information security, and regulatory compliance. She assists her clients with diligence and care, while identifying potential privacy vulnerabilities and conducting information security risk assessments. Tamara is a law graduate from Ono Academic College with a LLB in Law. She is a Fordham Law School graduate with a LLM in Intellectual Property and Information Technology. Tamara is a member of the State Bar of New York.

THOUGHTS? COMMENTS?

We are always looking to make this newsletter better, as such, we hope you like the new format of the newsletter. As always, comments and suggestions are always welcome. You can send your feedback to paulanocom@aol.com.

You are currently subscribed to the American Bar Association's E-Privacy Law Committee mailing list. Your e-mail address will only be used within the ABA and its entities. We do not sell or rent e-mail addresses to anyone outside the ABA.

Update your profile | Unsubscribe | Privacy Policy

American Bar Association: 321 North Clark Street | Chicago, IL 60654 | 800-285-2221
Copyright © 2018 ABA, All Rights Reserved.