USA - HEARST REACHES $50 MILLION MAGAZINE SUBSCRIBER DATA PRIVACY SETTLEMENT

Hearst Communications Inc reached a $50 million settlement of a lawsuit claiming it violated Michigan privacy law by selling its magazine subscribers’ personal information to third parties without consent.

Lawyers for the subscribers called the proposed class-action settlement the largest of its kind, triple the $16.375 million accord reached in April by Consumers Union, which publishes Consumer Reports.

Hearst was accused of violating the Michigan Video Rental Privacy Act by selling readers’ magazine subscription histories and reading habits to data mining companies, and then selling “enhanced” customer profiles containing data from those companies to third parties.

Read more: Reuters - Hearst reaches $50 million magazine subscriber data privacy settlement

USA - TEXAS CANCER CENTER REQUIRED TO PAY $4.3 MILLION IN PENALTIES FOR HIPAA VIOLATIONS

A U.S. Department of Health and Human Services Administrative Law Judge (ALJ) has ruled that The University of Texas MD Anderson Cancer Center (MD Anderson) violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and granted summary judgment to the Office for Civil Rights (OCR) on all issues, requiring MD Anderson to pay $4,348,000 in civil money penalties to OCR. This is the second summary judgment victory in OCR’s history of HIPAA enforcement and the $4.3 million is the fourth largest
amount ever awarded to OCR by an ALJ or secured in a settlement for HIPAA violations.

MD Anderson is both a degree-granting academic institution and a comprehensive cancer treatment and research center located at the Texas Medical Center in Houston. OCR investigated MD Anderson following three separate data breach reports in 2012 and 2013 involving the theft of an unencrypted laptop from the residence of an MD Anderson employee and the loss of two unencrypted universal serial bus (USB) thumb drives containing the unencrypted electronic protected health information (ePHI) of over 33,500 individuals. OCR’s investigation found that MD Anderson had written encryption policies going as far back as 2006 and that MD Anderson’s own risk analyses had found that the lack of device-level encryption posed a high risk to the security of ePHI.

Read more: HHS - Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations

USA - CALIFORNIA ENACTS SWEEPING NEW PRIVACY LEGISLATION

For any company that has assets in California or handles Californians’ personal information — regardless of the company’s location — California’s new Consumer Privacy Act of 2018 will likely have a significant impact on core business operations. That’s true whether your business is based in New York, Europe or Asia.

The law, which takes effect in 2020, gives consumers sweeping control over their personal data. It grants them the right to know what information companies like Facebook and Google are collecting, why they are collecting it, and who they are sharing it with. Consumers will have the option of barring tech companies from selling their data, and children under 16 must opt into allowing them to even collect their information at all.

The Act will apply to for-profit businesses that collect and control California residents’ personal information, do business in the State of California, and: (a) have annual gross revenues in excess of $25 million; or (b) receive or disclose the personal information of 50,000 or more California residents, households or devices on an annual basis; or (c) derive 50 percent or more of their annual revenues from selling California residents’ personal information.

While the law technically applies only to California residents, it will most likely have much broader implications. Most major companies that deal in consumer data have some Californian customers. That will leave those companies with two main options: either reform their global data protection and data rights infrastructures to comply with California’s law, or institute a patchwork data regime in which Californians are treated one way and everyone else another. That last option can be more expensive for companies and could disgruntle non-Californian customers should they be given fewer data privacy options by the service provider.

Read more: Bill Text - AB-375

Wall Street Journal - California Passes Sweeping Data-Privacy Bill

New York Law Journal - Understanding California’s Game-Changing Data Protection Law and its Global Impact

New York Times - California Passes Sweeping Law to Protect Online Privacy

CNN Money - California passes strictest online privacy law in the country
USA – CALIFORNIA COMPANY SETTLES FTC CHARGES RELATED TO PRIVACY SHIELD PARTICIPATION

A California company has agreed to settle Federal Trade Commission allegations that it falsely claimed it was in the process of being certified as complying with the EU-U.S. Privacy Shield framework, which establishes a process to allow companies to transfer consumer data from European Union countries to the United States in compliance with EU law. This is the FTC’s fourth case enforcing Privacy Shield.

According to the FTC’s complaint, the Commission alleges that ReadyTech Corporation, which provides online training services, falsely claimed on its website that it is “in the process of certifying that we comply with the U.S.-E.U. Privacy Shield Framework.”

While ReadyTech initiated an application to the U.S. Department of Commerce in October 2016, the company did not complete the steps necessary to participate in the Privacy Shield framework. The Department of Commerce administers the framework, while the FTC enforces the promises companies make when joining the Privacy Shield. The FTC alleged in its complaint that the company’s false claim that it is in the process of certification violates the FTC Act’s prohibition against deceptive acts or practices.

Read more: Press Release - California Company Settles FTC Charges Related to Privacy Shield Participation

USA – HOMELAND SECURITY SUBPOENAS TWITTER FOR DATA BREACH FINDER'S ACCOUNT

Homeland Security has served Twitter with a subpoena, demanding the account information of a data breach finder, credited with finding several large caches of exposed and leaking data. The New Zealand national, whose name isn't known but goes by the handle Flash Gordon, revealed the subpoena in a tweet.

The pseudonymous data breach finder regularly tweets about leaked data found on exposed and unprotected servers. Last year, he found a trove of almost a million patients' data leaking from a medical telemarketing firm. A recent find included an exposed cache of law enforcement data by ALERRT, a Texas State University-based organization, which trains police and civilians against active shooters. The database, secured in March but reported last week, revealed that several police departments were under-resourced and unable to respond to active shooter situations.

Homeland Security's export control agency, Immigration and Customs Enforcement (ICE), served the subpoena to Twitter on April 24, demanding information about the data breach finder's account.

Twitter informed him of the subpoena, per its policy on disclosing legal processes to its users. A legal effort to challenge the subpoena by a June 20 deadline was unsuccessful.

Read more: ZDNet - Homeland Security subpoenas Twitter for data breach finder's account

USA - NYDFS CYBERSECURITY REGULATION TO APPLY TO CONSUMER REPORTING AGENCIES

Governor Andrew M. Cuomo announced on 25 June 2018 that the Department of Financial Services has issued a final regulation to protect New Yorkers from the threat of data breaches at credit reporting agencies, such as the
Equifax breach that exposed the personal private data of millions of New Yorkers. The new regulation, which incorporates comments received during a public comment period, requires credit reporting agencies with significant operations in New York to register with DFS for the first time and to comply with New York's first-in-the-nation cybersecurity standard. The annual reporting obligation also provides the DFS Superintendent with the authority to deny, suspend and potentially revoke a consumer credit reporting agency's authorization to do business with New York's regulated financial institutions and consumers if the agency is found to be out of compliance with certain prohibited practices, including engaging in unfair, deceptive or predatory practices.

"As the federal government weakens consumer protections, New York is strengthening them with these new standards," Governor Cuomo said. "Oversight of credit reporting agencies ensures that the personal private information of New Yorkers is less vulnerable to the threat of cyber-attacks, providing them with peace of mind about their financial future."

Under the new regulation, all consumer credit reporting agencies that reported on 1,000 or more New York consumers in the preceding year must register annually with DFS beginning on or before September 1, 2018, and by February 1 of each successive year for the calendar year thereafter. The registration form must include an agency's officers and directors who will be responsible for compliance with the financial services, banking, and insurance laws, and regulations.

The DFS's cybersecurity regulation requires banks, insurance companies, and other financial services institutions regulated by DFS to have a cybersecurity program designed to protect consumers' private data; a written policy or policies that are approved by the board or a senior officer; a Chief Information Security Officer to help protect data and systems; and controls and plans in place to help ensure the safety and soundness of New York's financial services industry. DFS's cybersecurity regulation also requires the protection of data from third-party vendors and the filing with DFS of an annual certification of compliance.

Read more: New York State Press Release - Governor Cuomo Announces Action to Protect New Yorkers' Private Information Held by Credit Reporting Companies

**USA – EQUIFAX ENTERS INTO CONSENT ORDER WITH STATE BANKING REGULATORS REGARDING 2017 DATA BREACH**

Financial Services Superintendent Maria T. Vullo announced on 27 June 2018 that Equifax Inc. has agreed to take corrective actions following the company’s massive 2017 data breach under a consent order with the New York State Department of Financial Services (DFS) and the commissioners of seven other state banking regulators.

Under the consent order, Equifax must take corrective actions that include developing a proper risk assessment and improving the Board's oversight of information security information, audit, patch management, information technology operations, vendor management, and other functions. Equifax must also submit to the multi-state regulatory agencies for review a list of all remediation projects planned, in process or implemented in response to the 2017 breach, along with the company’s prioritization of those projects, as well as provide written reports to DFS and the other state regulators outlining its progress toward complying with each provision of the consent order.

DFS led the multi-state examination team on matters related to cybersecurity and internal audit functions. In addition to DFS, the multi-state team of regulators was comprised of the Alabama State Banking Department, the California Department of Business Oversight, the Georgia Department of Banking and Finance, the Maine Bureau
of Consumer Credit Protection, the Massachusetts Division of Banks, the North Carolina Office of Commissioner of Banks, and the Texas Department of Banking.


USA - SUPREME COURT HOLDS WARRANT REQUIRED TO OBTAIN HISTORICAL CELL PHONE LOCATION INFORMATION

On June 22, 2018, the United States Supreme Court held in Carpenter v. United States that law enforcement agencies must obtain a warrant supported by probable cause to obtain historical cell-site location information (“CSLI”) from third-party providers.

The government argued in Carpenter that it could access historical CSLI through a court order alone under the Stored Communications Act (the “SCA”). Under 18 U.S.C. § 2703(d), obtaining an SCA court order for stored records only requires the government to “offer specific and articulable facts showing that there are reasonable grounds.” However, in a split 5-4 decision, the Supreme Court held that the Fourth Amendment requires law enforcement agencies to obtain a warrant supported by probable cause to obtain historical CSLI.

Read more: Hunton Blog - Supreme Court Holds Warrant Required to Obtain Historical Cell Phone Location Information

USA - INDIVIDUAL CHARGED IN CONNECTION WITH THEFT OF CLASSIFIED MATERIAL FROM THE CENTRAL INTELLIGENCE AGENCY

On June 18, 2018, the U.S. Department of Justice charged a former CIA officer, Joshua Adam Schulte, 29, with stealing the CIA’s offensive malware tools and practices in 2016 and giving them to WikiLeaks.

A superseding 13-count indictment against Schulte includes such charges as illegally gathering and transmitting both lawfully and unlawfully gathered national defense information, hacking, stealing government property, sharing harmful computer programs, obstructing justice and making false statements.

"Schulte also intentionally caused damage without authorization to a CIA computer system by granting himself unauthorized access to the system, deleting records of his activities, and denying others access to the system," the Justice Department says. "Schulte subsequently made material false statements to FBI agents concerning his conduct at the CIA."

The charges against Schulte collectively carry a maximum prison sentence of 135 years. The crimes were allegedly committed in Virginia.

"Joshua Schulte, a former employee of the CIA, allegedly used his access at the agency to transmit classified material to an outside organization," says Manhattan U.S. Attorney Geoffrey S. Berman.

Read more: Department of Justice Press Release / Indictment
USA - FBI SEIZED CONTROL OF BOTNET LINKED TO RUSSIAN HACKING GROUP

On May 23, 2018 Federal Magistrate Judge Lisa Pupo Lenihan in Pittsburgh issued a warrant directing the domain registration firm Verisign to hand the ToKnowAll.com.com address over to the FBI pursuant to the FBI's investigation of "unauthorized intrusions being perpetrated by a group known to private cybersecurity investigators as the 'Sofacy Group' [...] a cyber-espionage group believed to have originated in Russia." The Sofacy Group allegedly targets government, military, and security organizations.

The FBI said it has been tracking the router malware since last August and, by seizing control of the domain, would be able to sinkhole the domain and at least partially block attackers’ control of the infected routers, as well as to identify infected routers.

At least 500,000 aging routers, mostly located in Ukraine, have been infected with malware that experts believe could be used to turn them into a massive botnet capable of launching a major cyberattack aimed, in part, at disrupting power grids.

"This operation is the first step in the disruption of a botnet that provides the Sofacy actors with an array of capabilities that could be used for a variety of malicious purposes, including intelligence gathering, theft of valuable information, destructive or disruptive attacks, and the misattribution of such activities," said U.S. Assistant Attorney General for National Security John C. Demers.

Read more: Warrant of Seizure / Affidavit in Support of the Warrant of Seizure

USA - CANADIAN HACKER-FOR-HIRE WHO CONSPIRED WITH AND AIDED RUSSIAN FSB OFFICERS SENTENCED TO FIVE YEARS IN PRISON

On May 29, 2018 U.S. District Judge Vince Chhabria in California sentenced a Canadian citizen and resident to serve five years in prison and to pay a fine that encompasses all of his remaining assets. Karim Baratov, 23, received a U.S. federal prison sentence after he admitted to working for alleged Russian intelligence officers who have been tied to a massive breach of search giant Yahoo in 2014.

Following a 47-count indictment filed in February 2017 and unsealed in March 2017, Mr. Baratov pled guilty in November 2017 to multiple charges including violating the U.S. Computer Fraud and Abuse Act and aggravated identity theft. The also indictment charges various suspects, including Mr. Baratov, with computer hacking, economic espionage and other criminal offenses tied in part to a 2014 hack attack against Yahoo that exposed at least 500 million accounts.

Russian citizen Alexsey Belan, 30, was charged with helping Dmitry Aleksandrovich Dokuchaev, 34, and Igor Anatolyevich Sushchin, 44, both alleged to be FSB agents, hack into Yahoo accounts from 2014 to 2016. All three have been charged with compromising Yahoo's network and gaining the ability to access Yahoo accounts. Belan was also designated as being subject to sanctions per a presidential executive order dated Dec. 29, 2016.

Belan and Baratov "were charged in a computer hacking conspiracy in which the two Russian FSB officers hired criminal hackers to collect information through computer intrusions in the United States and abroad, which resulted in the unauthorized access of Yahoo's network and the spear-phishing of webmail accounts at other service providers between January 2014 and December 2016," the Justice Department says.
"It's difficult to overstate the unprecedented nature of this conspiracy, in which members of a foreign intelligence service directed and empowered criminal hackers to conduct a massive cyber-attack against 500 million [victims'] user accounts," said John F. Bennett, the special agent in charge of the FBI's San Francisco field office, which led the investigation that resulted in the charges brought against Baratov.

"As part of his plea agreement, Baratov not only admitted to his hacking activities on behalf of his co-conspirators in the FSB, but also to hacking more than 11,000 webmail accounts on behalf of the FSB conspirators and other customers from in or around 2010 until his March 2017 arrest by Canadian authorities," the Justice Department said.

Baratov also agreed to pay restitution to his victims, as well as a fine of up to $2.25 million - $250,000 per count - up to a maximum of all assets that he has remaining.

Read more: Department of Justice Press Release / Indictment

**UPCOMING EVENTS**

**Bumps in the Night: Cybersecurity Legal Requirements, Government Enforcement, and Litigation**

Format: Webinar  
Date: July 18, 2018  
Time: 1:00 PM - 2:30 PM ET  
Credits: 1.50 General CLE Credit Hours  
Panelists: Esther Chavez, Ian C Ballon, Linda Holleran Kopp, Thomas J Smedinghoff  
Moderator: Ruth Hill Bro

Every business (and law firm) is a target and must protect confidential, sensitive, and valuable data from cyberattacks. The law requires it. The bottom line depends on it. But what is required—both legally and practically? What are the legal consequences for failing to do so? Join us as we explore these issues.

Social media profiles, financial information, patient records, confidential client information, and mission-critical data are among the common casualties in growing numbers of data breaches across the country. This is a phenomenon that does not discriminate: it touches all businesses, whether retailers, information brokers, financial institutions, media giants, universities, government agencies, healthcare companies, or law firms. Yet many have a false sense of security that somehow they are immune, that the IT Department has it handled, or that there is no reason to fear malware, ransomware, phishing attacks, or other things that go bump in the night.

Every business (and law firm) is a target and must protect confidential, sensitive, and valuable data from cyberattacks. The law requires it. The bottom line depends on it. But what is required—both legally and practically? What are the legal consequences for failing to do so? Join us as we explore these issues.

Join us to discover:
- The expanding legal obligations of every business and lawyer to provide appropriate or reasonable security and to disclose breaches
- Key developments in data breach and cybersecurity litigation
Emerging enforcement trends and lessons to be learned from recent FTC and State Attorney General enforcement

Practical takeaways for meeting cybersecurity legal requirements and avoiding enforcement and litigation

Programs can be taken either individually or part of the five-part series; there is a discount for registrants taking all. Read more here.

Ethics 101: Attorneys' Duties for Safeguarding Confidential Information on the Cloud

Format: Webinar
Date: July 31, 2018
Time: 1:00 PM - 2:30 PM ET
Credits: 1.50 Ethics/Professionalism CLE Credit Hours
Panelists: Catherine Sanders Reach, John Simek, Lucian T Pera, Sharon D Nelson

Most lawyers are using the cloud to store data even if they don’t realize it. Web-based e-mail is in the cloud. Office 365 data is in the cloud. Many of the software applications that lawyers rely on to run their practices are in the cloud.

But do clouds leak data? Assuredly they do, sometimes with scary regularity. No wonder lawyers worry about the potential ethical pitfalls of cloud computing, especially given the changes to ethical rules regarding competence with technology and the duty to safeguard confidential data. All attorneys seem to know that there is a prevailing reasonableness standard for vetting and using cloud providers, but lawyers struggle to understand what "reasonableness" means in the real world.

The panelists will explain the threats presented by cloud computing as well the benefits—and help you understand how to use cloud computing ethically. Read more here.

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.

**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]