May 2017

This Client Alert is a monthly update on privacy and cybersecurity developments as posted on Hunton & Williams' Privacy and Information Security Law Blog. If you would like to receive email alerts when new posts are published, please visit our blog and enter your email address in the subscribe field.

Recent posts on the Privacy and Information Security Law blog include:

- Belgian Privacy Commission Releases 2016 Annual Activity Report
- Amended Oregon Law Reinforces Importance of Adhering to Privacy Policies
- Privacy Shield First Annual Joint Review to Take Place in September 2017
- Bavarian DPA Tests GDPR Implementation of 150 Companies
- Target and State Attorneys General Resolve Investigation with Largest Multi-State Breach Settlement to Date
- New York AG Settles with Wireless Lock Maker Over Security Flaws
- China Releases Revised Draft on Measures for Implementation of the New Cybersecurity Law
- OCR Fines Texas Health System For Alleged HIPAA Privacy Rule Violation
- Global Ransomware Attacks Raise Key Legal Considerations
- Chinese Hackers Fined for Hack of New York Law Firms
- President Trump Signs Executive Order on Cybersecurity
- Second Circuit Affirms Dismissal of Putative Data Breach Class Action for Lack of Article III Standing
- Securing a Successful Transaction through Focused Privacy and Data Security Due Diligence
- China Publishes Final Measures for Security Reviews of Network Products and Services
- Wireless Provider Reaches $2.5 Million Settlement with OCR

Belgian Privacy Commission Releases 2016 Annual Activity Report
May 31, 2017

On May 26, 2017, the Belgian Privacy Commission (the "Belgian DPA") published its Annual Activity Report for 2016 (the "Annual Report") highlighting its main accomplishments from the past year. Continue Reading…

Amended Oregon Law Reinforces Importance of Adhering to Privacy Policies
May 31, 2017

On May 25, 2017, Oregon Governor Kate Brown signed into law H.B. 2090, which updates Oregon's Unlawful Trade Practices Act by holding companies liable for making misrepresentations on their websites (e.g., in privacy policies) or in their consumer agreements about how they will use, disclose, collect, maintain, delete or dispose of consumer information. Pursuant to H.B. 2090, a company engages in an unlawful trade practice if it makes assertions to consumers regarding the handling of their information that are materially inconsistent with its actual practices. Consumers can report violations to the Oregon Attorney General's consumer complaint hotline. H.B. 2090 reinforces the significance of carefully drafting clear, accurate privacy policies and complying with those policies' provisions.

Privacy Shield First Annual Joint Review to Take Place in September 2017
May 30, 2017

On May 29, 2017, a high-level EU Commission official and *Politico* reported that the primary objective of the first annual joint review of the EU-U.S. Privacy Shield ("Privacy Shield") is not to obtain more concessions from the U.S. regarding Europeans' privacy safeguards, but rather to monitor the current U.S. administration's work and steer U.S. privacy debates to prevent privacy safeguards from deteriorating. On March 31, 2017, the EU Commissioner for Justice, Věra Jourová, announced that the joint review will take place in September 2017. Continue Reading…

Bavarian DPA Tests GDPR Implementation of 150 Companies
May 24, 2017

On May 24, 2017, the Bavarian Data Protection Authority ("DPA") published a questionnaire to help companies assess their level of implementation of the EU General Data Protection Regulation ("GDPR"). Continue Reading…

Target and State Attorneys General Resolve Investigation with Largest Multi-State Breach Settlement to Date
May 24, 2017

On May 23, 2017, various attorneys general of 47 states and the District of Columbia announced that they had reached an $18.5 million settlement with Target regarding the states' investigation of the company's 2013 data breach. This represents the largest multi-state data breach settlement achieved to date. Continue Reading…

New York AG Settles with Wireless Lock Maker Over Security Flaws
May 23, 2017

On May 22, 2017, New York Attorney General Eric T. Schneiderman announced that the AG's office has reached a settlement (the "Settlement") with Safetech Products LLC ("Safetech") regarding the company's sale of insecure Bluetooth-enabled wireless doors and padlocks. In a press release, Schneiderman indicated that this "marks the first time an attorneys general's office has taken legal action against a wireless security company for failing to protect their [customers'] personal and private information." Continue Reading…

China Releases Revised Draft on Measures for Implementation of the New Cybersecurity Law
May 20, 2017

On May 19, 2017, the Cyberspace Administration of China ("CAC") issued a revised draft (the "Revised Draft") of its Measures for the Security Assessment of Outbound Transmission of Personal Information and Critical Data. The original draft was issued in April 2017, and similar to the original draft, the Revised Draft does not have the impact of law; it does, however, provide an indication of how the CAC's views on the Cybersecurity Law have evolved since the publication of the original draft. The Revised Draft was issued after the CAC received comments on the original draft from numerous parties. Continue Reading…

OCR Fines Texas Health System For Alleged HIPAA Privacy Rule Violation
May 17, 2017

On May 10, 2017, the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") announced a $2.4 million civil monetary penalty against Memorial Hermann Health System ("MHHS") for

alleged violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule. Continue Reading…

Global Ransomware Attacks Raise Key Legal Considerations
May 16, 2017

On May 12, 2017, a massive ransomware attack began affecting tens of thousands of computer systems in over 100 countries. The ransomware, known as "WannaCry," leverages a Windows vulnerability and encrypts files on infected systems and demands payment for their release. If payment is not received within a specified time frame, the ransomware automatically deletes the files. A wide range of industries have been impacted by the attack, including businesses, hospitals, utilities and government entities around the world. Continue Reading…

Chinese Hackers Fined for Hack of New York Law Firms
May 16, 2017

On May 5, 2017, the U.S. District Court for the Southern District of New York entered a default judgment in favor of the SEC against three Chinese defendants accused of hacking into the nonpublic networks of two New York-headquartered law firms and stealing confidential information regarding several publicly traded companies engaged in mergers and acquisitions. The defendants allegedly profited illegally by trading the stolen nonpublic information. After the defendants failed to answer the SEC's complaint, the court entered a default judgment against them, imposing a fine of approximately $8.9 million against the defendants (three times the profits they gained by the unlawful trading, the maximum penalty allowable under the relevant section of the Securities Exchange Act of 1934).

President Trump Signs Executive Order on Cybersecurity
May 11, 2017

On May 11, 2017, President Trump signed an executive order (the "Order") that seeks to improve the federal government's cybersecurity posture and better protect the nation's critical infrastructure from cyber attacks. The Order also seeks to establish policies for preventing foreign nations from using cyber attacks to target American citizens. Read the full text of the Order.

Second Circuit Affirms Dismissal of Putative Data Breach Class Action for Lack of Article III Standing
May 10, 2017

On May 2, 2017, the United States Court of Appeals for the Second Circuit issued a summary order affirming dismissal of a putative data breach class action against Michaels Stores, Inc. ("Michaels"). The plaintiff's injury theories were as follows: (1) the plaintiff's credit card information was stolen and twice used to attempt fraudulent purchases; (2) the risk of future identity fraud and (3) lost time and money resolving the attempted fraudulent charges and monitoring credit. The plaintiff, however, quickly cancelled her card after learning of the unauthorized charges and did not allege that she was held responsible for any of those charges. Continue Reading…

Securing a Successful Transaction through Focused Privacy and Data Security Due Diligence
May 4, 2017

Privacy and data security issues have become the subject of critical focus in corporate mergers, acquisitions, divestitures and related transactions. In 2016 and 2017, several large transactions,

especially those involving telecommunications, entertainment and technology companies, have been impacted by either concerns about the collection and use of personal information or significant information security breaches. The FTC has sharpened its focus on the use of personal information as a factor in evaluating the competitive effects of a given corporate transaction, and the SEC is now closely scrutinizing privacy and data security representations made to investors in public filings connected to transactions. More broadly, privacy and data security problems that are not timely discovered before entering into an M&A transaction can become significant liabilities post-closing and also lead to litigation. Continue Reading…

China Publishes Final Measures for Security Reviews of Network Products and Services
May 3, 2017

On May 2, 2017, the Cyberspace Administration of China published the final version of the *Measures for the Security Review of Network Products and Services* (for trial implementation) (the "Measures"), after having published a draft for public comment in February. Pursuant to the Cybersecurity Law of China (the "Cybersecurity Law"), if an operator of key information infrastructure purchases a network product or service that may affect national security, a security review of that product or service is required. The Measures provide detailed information about how these security reviews will actually be implemented. The Measures will come into effect on June 1, 2017, together with the Cybersecurity Law. The Measures should not be confused with the final version of the draft *Measures for the Security Assessment of Outbound Transmission of Personal Information and Critical Data*, which was published on April 11, 2017, and remain open for public comment. Continue Reading…

Wireless Provider Reaches $2.5 Million Settlement with OCR
May 1, 2017

On April 24, 2017, the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") announced that it had entered into a resolution agreement with CardioNet, Inc. ("CardioNet") stemming from gaps in policies and procedures uncovered after CardioNet reported breaches of unsecured electronic protected health information ("ePHI"). CardioNet provides patients with an ambulatory cardiac monitoring service, and the settlement is OCR's first with a wireless health services provider. Continue Reading…

Visit our award-winning Privacy and Information Security Law Blog at www.huntonprivacyblog.com for global privacy and cybersecurity law updates and analysis.