

PRIVACY & INFORMATION SECURITY LAW BLOG

Global Privacy and Cybersecurity Law Updates and Analysis



June 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:

- [Ransomware Health Data Breach Affects 500,000 Patients](#)
- [Information Security 101 with Lisa Sotto: Legal Risks](#)
- [Record Data Breach Settlement in Anthem Class Action](#)
- [Tempur Sealy Data Breach: Putative Class Action Filed](#)
- [Implementation of the EU GDPR: 30-Minute Guidance Review](#)
- [UK ICO Revises Subject Access Guidance Following Court Rulings](#)
- [FTC Releases Guidance on COPPA Compliance](#)
- [Germany Issues Ethics Report on Automated and Connected Cars](#)
- [UK Government Confirms Implementation of EU GDPR](#)
- [South Korea Joins the APEC Cross-Border Privacy Rules System](#)
- [OCR and Health Care Industry Cybersecurity Task Force Publish Cybersecurity Materials](#)
- [China Releases Draft Guidelines on Cross-Border Data Transfers Pursuant to the Cybersecurity Law](#)
- [Federal Court Imposes Record Fine on TV Provider for Do Not Call Violations](#)
- [European Commission Pushes for Greater EU Role in Cybersecurity](#)
- [EU Commission Issues Questionnaire in Preparation for Annual Review of Privacy Shield](#)
- [Washington Becomes Third State to Enact Biometric Privacy Law](#)
- [Cybersecurity Law Goes Into Effect in China](#)
- [Colorado Publishes Cybersecurity Regulations for Financial Institutions](#)
- [UK ICO Stresses Importance of Preparing for the GDPR and Addresses the ICO's Role Post-Brexit](#)

Ransomware Health Data Breach Affects 500,000 Patients June 30, 2017

On June 26, 2017, Airway Oxygen, a provider of oxygen therapy and home medical equipment, [reported](#) that it was the subject of a ransomware attack affecting 500,000 patients' protected health information. The attack is the second largest health data breach [recorded](#) by the Office for Civil Rights ("OCR") this year, and the largest ransomware incident recorded by OCR since it began tracking incidents in 2009. [Continue Reading...](#)

Information Security 101 with Lisa Sotto: Legal Risks June 29, 2017

In the first segment of this three-part series, [Lisa Sotto](#), head of the [Global Privacy and Cybersecurity practice](#) at Hunton & Williams, discusses information security law issues with The Electronic Discovery Institute. "[Information security] is a significant risk issue" and should be "at the top of the radar screen" for C-suites and boards of directors, says Sotto. In this segment, Sotto addresses U.S. and global data breach notification laws.

[Watch the full video.](#)

Record Data Breach Settlement in Anthem Class Action June 26, 2017

On June 23, 2017, Anthem Inc., the nation's second largest health insurer, reached a record \$115 million [settlement](#) in a class action lawsuit arising out of a 2015 data breach that exposed the personal information of more than 78 million people. Among other things, the settlement creates a pool of funds to provide credit monitoring and reimbursement for out-of-pocket costs for customers, as well as up to \$38 million in attorneys' fees. [Continue Reading...](#)

Tempur Sealy Data Breach: Putative Class Action Filed June 26, 2017

On June 12, 2017, a putative class action was [filed](#) in the U.S. District Court for the Northern District of Georgia against Tempur Sealy International, Inc. and Aptos, Inc. Tempur Sealy is a mattress, bedding and pillow retailer based in Lexington, Kentucky. Aptos is headquartered in Atlanta, Georgia, and formerly hosted and maintained Tempur Sealy's website and online payment system. The plaintiff alleges that the breach was discovered in November of 2016 and involved the exposure of payment card data and other PII of an undisclosed number of Tempur Sealy customers. [Continue Reading...](#)

Implementation of the EU GDPR: 30-Minute Guidance Review June 26, 2017

As companies in the EU and the U.S. prepare for the application of the EU General Data Protection Regulation ("GDPR") in May 2018, Hunton & Williams' Global Privacy and Cybersecurity partner [Aaron Simpson](#) discusses the key, significant changes from the EU Directive that companies must comply with before next year. Accountability, expanded data subject rights, breach notification, sanctions and data transfer mechanisms are a few requirements that Simpson explores in detail. He reminds companies that, in the coming year, it will be very important to "monitor...and stay aware of the guidance being produced by regulators," but also that the guidance is not a substitute for the specific preparations that each business will need to perform in order to comply with the GDPR.

[Listen to the full 30-minute webinar.](#)

UK ICO Revises Subject Access Guidance Following Court Rulings June 23, 2017

On June 20, 2017, the UK Information Commissioner's Office ("ICO") published an updated version of its [Code of Practice on Subject Access Requests](#) (the "Code"). The updates are primarily in response to three Court of Appeal decisions from earlier this year regarding data controllers' obligations to respond to subject access requests ("SARs"). The revisions more closely align the ICO's position with the court's judgments. [Continue Reading...](#)

FTC Releases Guidance on COPPA Compliance June 22, 2017

On June 21, 2017, the Federal Trade Commission updated its guidance, [Six-Step Compliance Plan for Your Business](#), for complying with the Children's Online Privacy Protection Act ("COPPA"). The FTC enforces the COPPA Rule, which sets requirements regarding children's privacy and safety online. The

updated guidance adds new information on situations where COPPA applies and steps to take for compliance. [Continue Reading...](#)

Germany Issues Ethics Report on Automated and Connected Cars June 22, 2017

On June 20, 2017, the German Federal Ministry of Transport and Digital Infrastructure issued a [report](#) on the ethics of Automated and Connected Cars (the “Report”). The Report was developed by a multidisciplinary Ethics Commission established in September 2016 for the purpose of developing essential ethical guidelines for the use of automated and connected cars. [Continue Reading...](#)

UK Government Confirms Implementation of EU GDPR June 21, 2017

On June 21, 2017, in the [Queen’s Speech to Parliament](#), the UK government confirmed its intention to press ahead with the implementation of the EU General Data Protection Regulation (“GDPR”) into national law. Among the announcements on both national and international politics, the Queen stated that, “A new law will ensure that the United Kingdom retains its world-class regime protecting personal data, and proposals for a new digital charter will be brought forward to ensure that the United Kingdom is the safest place to be online.” The statement confirms the priority given to data protection issues by the UK government. The UK government specifically confirmed that a new data protection bill will be brought forward to implement the EU GDPR and the EU Directive, which applies to law enforcement data processing. By doing so, the UK government intends to maintain the highest standards of data protection to ensure that data flows with EU Member States and other countries of the world will be maintained after Brexit. The Information Commissioner’s Office’s powers and available sanctions will also be increased.

South Korea Joins the APEC Cross-Border Privacy Rules System June 12, 2017

On Monday, June 12, 2017, South Korea’s Ministry of the Interior and the Korea Communications Commission announced that South Korea has secured approval to participate in the APEC Cross-Border Privacy Rules (“CBPR”) system. South Korea had [submitted](#) its intent to join the CBPR system back in January 2017. South Korea will become the fifth APEC economy to join the CBPR system. The other four participants are Canada, Japan, Mexico and the United States. [Continue Reading...](#)

OCR and Health Care Industry Cybersecurity Task Force Publish Cybersecurity Materials June 12, 2017

The U.S. Department of Health and Human Services’ Office for Civil Rights (“OCR”) and the Health Care Industry Cybersecurity Task Force (the “Task Force”) have published important materials addressing cybersecurity in the health care industry. [Continue Reading...](#)

China Releases Draft Guidelines on Cross-Border Data Transfers Pursuant to the Cybersecurity Law June 9, 2017

On May 27, 2017, the National Information Security Standardization Technical Committee of China published draft guidelines on cross-border transfers pursuant to the new Cybersecurity Law, entitled *Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment* (the “Draft Guidelines”). The earlier draft, [Measures for the Security Assessment of Outbound Transmission of](#)

[Personal Information and Critical Data](#) (the “Draft Measures”), requires network operators to conduct “security assessments” when they propose to transfer personal information and “important information” to places outside of China. These “security assessments” are essentially audits of the cybersecurity circumstances surrounding the proposed transfer that are intended to produce an assessment of the risk involved. If the assessment indicates that the risk is too high, the transfer must be terminated. [Continue Reading...](#)

Federal Court Imposes Record Fine on TV Provider for Do Not Call Violations **June 8, 2017**

On June 5, 2017, an Illinois federal court [ordered](#) satellite television provider Dish Network LLC (“Dish”) to pay a record \$280 million in civil penalties for violations of the FTC’s Telemarketing Sales Rule (“TSR”), the Telephone Consumer Protection Act (“TCPA”) and state law. In its [complaint](#), the FTC alleged that Dish initiated, or caused a telemarketer to initiate, outbound telephone calls to phone numbers listed on the Do Not Call Registry, in violation of the TSR. The complaint further alleged that Dish violated the TSR’s prohibition on abandoned calls and assisted and facilitated telemarketers when it knew or consciously avoided knowing that telemarketers were breaking the law. [Continue Reading...](#)

European Commission Pushes for Greater EU Role in Cybersecurity **June 7, 2017**

On June 7, 2017, the European Commission published a paper signaling the EU’s intention to increase its role in directing cybersecurity policy and responses across its member states. The increasing threat posed by cyber attacks is highlighted in the EU Commission’s [Reflection Paper on the Future of European Defence](#), which builds its case for closer union in respect of defense efforts. [Continue Reading...](#)

EU Commission Issues Questionnaire in Preparation for Annual Review of Privacy Shield **June 5, 2017**

On June 2, 2017, in preparation for the first annual [review](#) of the EU-U.S. Privacy Shield (“Privacy Shield”) framework, the European Commission has sent questionnaires to trade associations and other groups, including the Centre for Information Policy Leadership at Hunton & Williams LLP, to seek information from their Privacy Shield-certified members on the experiences of such organizations during the first year of the Privacy Shield. The EU Commission intends to use the questionnaire responses to inform the annual review of the function, implementation, supervision and enforcement of the Privacy Shield. [Continue Reading...](#)

Washington Becomes Third State to Enact Biometric Privacy Law **June 1, 2017**

On May 16, 2017, the Governor of the State of Washington, Jay Inslee, signed into law [House Bill 1493](#) (“H.B. 1493”), which sets forth requirements for businesses who collect and use biometric identifiers for commercial purposes. The law will become effective on July 23, 2017. With the enactment of H.B. 1493, Washington becomes the third state to pass legislation regulating the commercial use of biometric identifiers. Previously, both Illinois and Texas enacted the Illinois Biometric Information Privacy Act ([740 ILCS 14](#)) (“BIPA”) and the Texas Statute on the Capture or Use of Biometric Identifier ([Tex. Bus. & Com. Code Ann. §503.001](#)), respectively. [Continue Reading...](#)

Cybersecurity Law Goes Into Effect in China

June 1, 2017

On June 1, 2017, the new [Cybersecurity Law](#) went into effect in China. This post takes stock of (1) which measures have been passed so far, (2) which ones go into effect on June 1 and (3) which ones are in progress but have yet to be promulgated. [Continue Reading...](#)

**Colorado Publishes Cybersecurity Regulations for Financial Institutions
June 1, 2017**

Recently, the Colorado Division of Securities (the “Division”) published [cybersecurity regulations](#) for broker-dealers and investment advisers regulated by the Division. Colorado’s cybersecurity regulations follow similar regulations [enacted in New York](#) that apply to certain state-regulated financial institutions. [Continue Reading...](#)

**UK ICO Stresses Importance of Preparing for the GDPR and Addresses the ICO’s Role Post-Brexit
June 1, 2017**

With just under one year to go before the EU General Data Protection Regulation (“GDPR”) becomes law across the European Union, the UK Information Commissioner’s Office (“ICO”) has continued its efforts to help businesses prepare for the new law. The ICO also has taken steps to address its own role post-Brexit. [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.