PRIVACY & INFORMATION SECURITY LAW BLOG
Global Privacy and Cybersecurity Law Updates and Analysis

June 2016

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:

- Article 29 Working Party and EDPS Release Opinions on the ePrivacy Directive
- OCR Settles Two HIPAA Cases with Public Health Centers in Oregon and Mississippi
- White House Releases New Policy on Federal Cyber Incident Response
- Lisa Sotto Interviewed on Privacy Piracy Radio Show
- U.S. Department of Commerce Launches Privacy Shield Website
- EU Regulators Will Not Challenge Adequacy of Privacy Shield for at Least One Year
- The EU-U.S. Privacy Shield: A How-To Guide
- CNIL Serves Formal Notice to Microsoft to Comply with French Data Protection Law
- Advocate General Finds Member States May Not Breach EU Laws Over Electronic Communications Retention
- Second Circuit Holds Microsoft Cannot Be Compelled to Turn Over Emails Stored Abroad
- FTC Issues Warning Letters to Companies Falsely Claiming APEC CBPR Certification
- European Commission Adopts Privacy Shield
- Second Draft of the Cybersecurity Law Published for Comment in China
- European Parliament Adopts Directive on Security of Network and Information Systems
- EU Commission Signs Agreement with Industry on Cybersecurity
- OCR Enters into First Enforcement Action Against Business Associate
- ICO Releases Annual Report for 2015-2016

Article 29 Working Party and EDPS Release Opinions on the ePrivacy Directive
July 29, 2016

On July 25, 2016, the Article 29 Working Party (the "Working Party") and the European Data Protection Supervisor ("EDPS") released their respective Opinions regarding the review of Directive 2002/58/EC on privacy and electronic communications (the "ePrivacy Directive"). Both the Working Party and the EDPS stressed that new rules should complement the protections available under the EU General Data Protection Regulation ("GDPR"). Continue Reading…

OCR Settles Two HIPAA Cases with Public Health Centers in Oregon and Mississippi
July 28, 2016

On July 21, 2016, the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") entered into resolution agreements with two large public health centers, Oregon Health & Science University ("OHSU") and the University of Mississippi Medical Center ("UMMC"), over alleged HIPAA violations. Continue Reading…

White House Releases New Policy on Federal Cyber Incident Response
July 28, 2016

On July 26, 2016, the White House unveiled Presidential Policy Directive PPD-41("PPD-41"), Subject: United States Cyber Incident Coordination, which sets forth principles for federal responses to cyber incidents approved by the National Security Council ("NCS"). Coming on the heels of several high-profile federal breaches, including the Office of Personnel Management's loss of security clearance information and the hack of over 700,000 IRS accounts, PPD-41 is a component of President Obama's Cybersecurity National Action Plan. PPD-41 first focuses on incident response to cyber attacks on government assets, but also outlines federal incident responses to cyber attacks on certain critical infrastructure within the private sector. Continue Reading…

Lisa Sotto Interviewed on Privacy Piracy Radio Show
July 27, 2016

On July 25, 2016, Lisa Sotto, partner and head of the Global Privacy and Cybersecurity practice at Hunton & Williams LLP, was interviewed on KUCI 88.9 FM radio's Privacy Piracy show. Lisa discussed the changing regulatory landscape, information security enforcement actions, the threat actors who attack companies' data and how to manage the aftermath of a data breach. "There is no industry sector that is exempt [from being targeted]," Lisa says. She notes that, because "data can be sold for a monetary sum, data is now the equivalent of cash."

Listen to the full interview.

U.S. Department of Commerce Launches Privacy Shield Website
July 26, 2016

On July 26, 2016, the U.S. Department of Commerce announced that it has launched a new website that provides individuals and companies with additional information regarding the EU-U.S. Privacy Shield Framework ("Privacy Shield"). Among other things, the website provides information about complying with, and self-certifying to, the Privacy Shield's principles. The Department of Commerce's website will begin accepting certifications on August 1, 2016.

EU Regulators Will Not Challenge Adequacy of Privacy Shield for at Least One Year
July 26, 2016

On July 26, 2016, Isabelle Falque-Pierrotin, the Chairwoman of the Article 29 Working Party of data protection regulators, announced that EU data protection regulators will not challenge the adequacy of the EU-U.S. Privacy Shield ("Privacy Shield") for at least one year (i.e., until after summer 2017). The European Commission is scheduled to conduct a mandatory review of the adequacy of the Privacy Shield by May 2017. Continue Reading…

The EU-U.S. Privacy Shield: A How-To Guide
July 26, 2016

On July 12, 2016, after months of negotiations and criticism, the EU-U.S. Privacy Shield ("Privacy Shield") was officially adopted by the European Commission and the Department of Commerce. Similar to the Safe Harbor, companies must certify their compliance with the seven principles comprising the Privacy Shield to use the Shield as a valid data transfer mechanism. Hunton & Williams partner Lisa J. Sotto and associate Chris D. Hydak recently published an article in *Law360* entitled "The EU-U.S. Privacy Shield: A How-To Guide." In the article, Lisa and Chris detail the Privacy Shield principles, the benefits of

certification, how the Shield will be enforced, and the challenges and risks associated with the future of the Privacy Shield.

Read the full article.

CNIL Serves Formal Notice to Microsoft to Comply with French Data Protection Law
July 26, 2016

On July 20, 2016, the French Data Protection Authority ("CNIL") announced that it issued a formal notice to Microsoft Corporation ("Microsoft") about Windows 10, ordering Microsoft to comply with the French Data Protection Act within three months.

Background

Following the launch of Microsoft's new operation system, Windows 10, in July 2015, the CNIL was alerted by the media and political parties that Microsoft could collect excessive personal data via Windows 10. A group composed of several EU data protection authorities was created within the Article 29 Working Party to examine the issue and conduct investigations in their relevant EU Member States. The CNIL initiated its investigation and carried out seven online inspections in April and June 2016. The CNIL also questioned Microsoft on certain points of its privacy statement. Continue Reading…

Advocate General Finds Member States May Not Breach EU Laws Over Electronic Communications Retention
July 20, 2016

On July 19, 2016, Advocate General Saugmandsgaard Oe ("Advocate General"),published his Opinion on two joined cases relating to data retention requirements in the EU, C-203/15 and C-698/15. These cases were brought following the Court of Justice for the European Union's ("CJEU's") decision in the *Digital Rights Ireland* case, which invalidated Directive 2006/24/EC on data retention. The two cases, referred from courts in Sweden and the UK respectively, sought to establish whether a general obligation to retain data is compatible with the fundamental rights to privacy and data protection under EU law. Continue Reading…

Second Circuit Holds Microsoft Cannot Be Compelled to Turn Over Emails Stored Abroad
July 20, 2016

On July 14, 2016, the U.S. Court of Appeals for the Second Circuit held that Microsoft Corporation ("Microsoft") cannot be compelled to turn over customer emails stored abroad to U.S. law enforcement authorities. Continue Reading…

FTC Issues Warning Letters to Companies Falsely Claiming APEC CBPR Certification
July 14, 2016

On July 14, 2016, the Federal Trade Commission issued warning letters to 28 companies relating to apparent false claims of participation in the APEC Cross-Border Privacy Rules ("CBPR").

The warning letters state that the companies' websites represent APEC CBPR certification even though the companies do not appear to have undertaken the necessary steps to claim certification, such as a review and approval process by an APEC-recognized Accountability Agent. Continue Reading…

European Commission Adopts Privacy Shield
July 12, 2016

On July 12, 2016, the EU Commissioner for Justice, Consumers and Gender Equality, Věra Jourová, and U.S. Secretary of Commerce Penny Pritzker announced the formal adoption of the EU-U.S. Privacy Shield (the "Privacy Shield") framework, composed of an Adequacy Decision and accompanying Annexes. Continue Reading…

Second Draft of the Cybersecurity Law Published for Comment in China
July 7, 2016

On July 5, 2016, the Standing Committee of the National People's Congress of the People's Republic of China (the "Standing Committee") published the full second draft of the Cybersecurity Law (the "second draft"). The publication of the second draft comes after the Standing Committee's second reading of the draft on June 27, 2016. The public may comment on the second draft of the Cybersecurity Law until August 4, 2016. Continue Reading…

European Parliament Adopts Directive on Security of Network and Information Systems
July 7, 2016

On July 6, 2016, the European Parliament adopted the Directive on Security of Network and Information Systems (the "NIS Directive"), which will come into force in August 2016. EU Member States will have 21 months to transpose the NIS Directive into their national laws. The NIS Directive is part of the European Commission's cybersecurity strategy for the European Union, and is designed to increase cooperation between EU Member States on cybersecurity issues. Continue Reading…

EU Commission Signs Agreement with Industry on Cybersecurity
July 6, 2016

On July 5, 2016, the European Commission announced the launch of a new public-private partnership (the "Partnership") on cybersecurity, as part of its Digital Single Market and EU Cybersecurity strategies. In this context, the European Commission released several documents, including a Commission Decision establishing a contractual arrangement of the new Partnership for cybersecurity industrial research, and a Staff Working Document on the preparation activities for the Partnership. Continue Reading…

OCR Enters into First Enforcement Action Against Business Associate
July 6, 2016

On June 30, 2016, the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") announced that it had settled potential HIPAA Security Rule violations with Catholic Health Care Services of the Archdiocese of Philadelphia ("CHCS"). This is the first enforcement action OCR has taken against a business associate since the HIPAA Omnibus Rule was enacted in 2013. The HIPAA Omnibus Rule made business associates directly liable for their violations of the HIPAA rules. The settlement with CHCS is also notable because it involved a breach that affected fewer than 500 individuals. Continue Reading…

ICO Releases Annual Report for 2015-2016
July 4, 2016

On June 28, 2016, the UK Information Commissioner's Office ("ICO") released its Annual Report for 2015-2016 (the "Report").

According to the Report, the ICO has dealt with an increase in the number of data protection concerns, handling 16,388 complaints in total. Particularly noteworthy is the £130,000 fine imposed on Pharmacy 2U for breach of the fair processing requirements under the UK Data Protection Act 1998. Pharmacy 2U sold details of over 20,000 customers to a list marketing company without customers' knowledge or consent. 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.