

PRIVACY & INFORMATION SECURITY LAW BLOG

Global Privacy and Cybersecurity Law Updates and Analysis



October 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:

- [Regulation on the Online Protection of Minors Published for Comment in China](#)
- [FCC Adopts Broadband Consumer Privacy Rules](#)
- [Privacy Blog Nominated for Best AmLaw Blog of 2016 – Please Vote To Help Us Win!](#)
- [Irish Privacy Advocacy Group Challenges EU-U.S. Privacy Shield](#)
- [APEC Cross-Border Privacy Rules System Poised for Expansion](#)
- [FTC Issues Guide for Businesses on Handling Data Breaches](#)
- [Court Rules Fraud Involving a Computer Is Not ‘Computer Fraud’ under Crime Protection Policy](#)
- [European Commission Proposes Changes to Data Export Decisions](#)
- [NHTSA Set to Release New Automobile Cybersecurity Best Practices](#)
- [Article 29 Working Party Issues Results of Fablab Workshop on the GDPR](#)
- [HHS Releases Guidance on HIPAA and Cloud Computing](#)
- [Federal Regulators Propose New Cybersecurity Rule for Big Banks](#)
- [CJEU Rules That Dynamic IP Addresses Are Personal Data](#)
- [California AG Announces Launch of Online CalOPPA Reporting Form](#)
- [CIPL and Telefónica Call for Action on New Approaches to Data Transparency](#)
- [UK ICO Seeks Personal Liability for Directors](#)
- [G-7 Endorses Best Practices for Bank Cybersecurity](#)
- [Texas AG Settles Suit with Messaging App Over Children’s Data Practices](#)
- [Department of Defense Finalizes Rule for Cyber Incident Reporting](#)
- [The Arc of a Data Breach: A 3-Part Series to Make Sure You’re Prepared](#)
- [CNIL Provides Update on Compliance Pack Regarding Connected Vehicles](#)
- [CIPL and its GDPR Project Stakeholders Discuss DPOs and Risk under GDPR](#)
- [EDPS Issues Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data](#)
- [CISPE Unveils Cloud Providers Code of Conduct](#)

Regulation on the Online Protection of Minors Published for Comment in China October 28, 2016

Recently, the Cyberspace Administration of China published for public comment a draft of the Regulations on the Online Protection of Minors (“Draft Regulations”). The Draft Regulations are open for comment until October 31, 2016. [Continue Reading...](#)

FCC Adopts Broadband Consumer Privacy Rules October 28, 2016

On October 27, 2016, the Federal Communications Commission (“FCC”) [announced](#) the adoption of rules that require broadband Internet Service Providers (“ISPs”) to take steps to protect consumer privacy (the “Rules”). According to the FCC’s [press release](#), the Rules are intended to “ensure broadband customers have meaningful choice, greater transparency and strong security protections for their personal information collected by ISPs.” [Continue Reading...](#)

Privacy Blog Nominated for Best AmLaw Blog of 2016 – Please Vote To Help Us Win! **October 27, 2016**

Hunton & Williams LLP is proud to announce our Privacy & Information Security Law Blog has been nominated in The Expert Institute's [2016 Best Legal Blog Contest](#) for Best AmLaw Blog of 2016. From all of the editors, lawyers and contributors that make our blog a success, we appreciate your continued support and readership, and ask that you please take a moment to [vote](#) for our blog!

Irish Privacy Advocacy Group Challenges EU-U.S. Privacy Shield **October 27, 2016**

A recent [update](#) on the Court of Justice of the European Union's (the "CJEU's") website has revealed that Digital Rights Ireland, an Irish privacy advocacy group, has filed an action for annulment against the European Commission's adequacy decision on the EU-U.S. Privacy Shield (the "Privacy Shield"). [Continue Reading...](#)

APEC Cross-Border Privacy Rules System Poised for Expansion **October 26, 2016**

On October 21, 2016, the Vietnam e-Commerce and Information Technology Agency and APEC co-hosted an APEC Cross-Border Privacy Rules ("CBPR") system capacity-building workshop in Da Nang, Vietnam, on the heels of last week's bilateral [affirmation of commitment](#) between the U.S. and Japan to implement and expand the CBPR system. The workshop further signals the continuing growth of the CBPR system. [Continue Reading...](#)

FTC Issues Guide for Businesses on Handling Data Breaches **October 26, 2016**

On October 25, 2016, the Federal Trade Commission [released](#) a guide for businesses on how to handle and respond to data breaches (the "Guide"). The [16-page Guide](#) details steps businesses should take once they become aware of a potential breach. The Guide also underscores the need for cyber-specific insurance to help offset potentially significant response costs. [Continue Reading...](#)

Court Rules Fraud Involving a Computer Is Not 'Computer Fraud' under Crime Protection Policy **October 25, 2016**

On October 18, 2016, the United States Court of Appeals for the Fifth Circuit [held](#) in *Apache Corp. v. Great American Ins. Co.*, No 15-20499 (5th Cir. Oct. 18, 2016), that a crime protection insurance policy does not cover loss resulting from a fraudulent email directing funds to be sent electronically to the imposter's bank account because the scheme did not constitute "computer fraud" under the policy. [Continue Reading...](#)

European Commission Proposes Changes to Data Export Decisions **October 24, 2016**

Earlier this month, at a [meeting](#) of the Article 31 Committee, the European Commission ("Commission") unveiled two draft Commission Implementing Decisions that propose amendments to the existing adequacy decisions and decisions on EU Model Clauses. [Continue Reading...](#)

NHTSA Set to Release New Automobile Cybersecurity Best Practices October 21, 2016

On October 14, 2016, the National Highway Transportation Administration (“NHTSA”) indicated in a [letter](#) to Congress that it intends to issue new best practices on vehicle cybersecurity. This letter came in response to an earlier [request](#) from the House Committee on Energy and Commerce (“Energy and Commerce Committee”) that NHTSA convene an industry-wide effort to develop a plan to address vulnerabilities posed to vehicles by On-Board Diagnostics (“OBD-II”) ports. [Continue Reading...](#)

Article 29 Working Party Issues Results of Fablab Workshop on the GDPR October 20, 2016

On October 7, 2016, the Article 29 Working Party (the “Working Party”) published a summary of the discussions that took place at its “Fablab” workshop entitled [GDPR/from concepts to operational toolbox, DIY](#), which took place on July 26, 2016, in Brussels. [Continue Reading...](#)

HHS Releases Guidance on HIPAA and Cloud Computing October 20, 2016

Earlier this month, the Department of Health and Human Services’ Office for Civil Rights [issued](#) guidance (the “Guidance”) for HIPAA-covered entities that use cloud computing services involving electronic protected health information (“ePHI”). [Continue Reading...](#)

Federal Regulators Propose New Cybersecurity Rule for Big Banks October 19, 2016

On October 19, 2016, the Federal Deposit Insurance Corporation (“FDIC”), the Federal Reserve System (the “Fed”) and Office of the Comptroller of the Currency issued an [advance notice of proposed rulemaking](#) suggesting new cybersecurity regulations for banks with assets totaling more than \$50 billion (the “Proposed Standards”). [Continue Reading...](#)

CJEU Rules That Dynamic IP Addresses Are Personal Data October 19, 2016

On October 19, 2016, the Court of Justice of the European Union (the “CJEU”) issued its judgment in [Patrick Breyer v. Bundesrepublik Deutschland](#), following the [Opinion](#) of Advocate General Manuel Campos Sánchez-Bordona on May 12, 2016. The CJEU followed the Opinion of the Advocate General and declared that a dynamic IP address registered by a website operator must be treated as personal data by that operator to the extent that the user’s Internet service provider (“ISP”) has – and may provide – additional data that in combination with the IP address that would allow for the identification of the user. [Continue Reading...](#)

California AG Announces Launch of Online CalOPPA Reporting Form October 19, 2016

On October 14, 2016, California Attorney General Kamala D. Harris [announced](#) the release of a publicly available [online form](#) that will enable consumers to report potential violations of the California Online

Privacy Protection Act (“CalOPPA”). CalOPPA requires website and mobile app operators to post a privacy policy that contains certain specific content. [Continue Reading...](#)

CIPL and Telefónica Call for Action on New Approaches to Data Transparency October 18, 2016

Recently, the [Centre for Information Policy Leadership](#) (“CIPL”) at Hunton & Williams LLP, a privacy and information policy think tank based in Brussels, London and Washington, D.C., and Telefónica, one of the largest telecommunications company in the world, issued a joint white paper on [Reframing Data Transparency](#) (the “white paper”). The white paper was the outcome of a June 2016 roundtable held by the two organizations in London, in which senior business leaders, Data Privacy Officers, lawyers and academics discussed the importance of user-centric transparency to the data driven economy. [Continue Reading...](#)

UK ICO Seeks Personal Liability for Directors October 17, 2016

On October 13, 2016, Elizabeth Denham, the UK Information Commissioner, suggested that directors of companies who violate data protection laws should be personally liable to pay fines at a House of Commons Public Bill Committee [meeting](#) when discussing the latest draft of the Digital Economy Bill (the “Bill”). The Bill is designed to enable businesses and individuals to access fast, digital communications services, promote investment in digital communications infrastructure and support the “digital transformation of government.” [Continue Reading...](#)

G-7 Endorses Best Practices for Bank Cybersecurity October 17, 2016

On October 11, 2016, Group of Seven (“G-7”) financial leaders endorsed the [Fundamental Elements of Cybersecurity for the Financial Sector](#) (“Best Practices”), a set of non-binding best practices for banks and financial institutions to address cybersecurity threats. The endorsement was motivated by recent large hacks on international banks, including the February 2016 theft of \$81 million from the central bank of Bangladesh’s account at the New York Federal Reserve. [Continue Reading...](#)

Texas AG Settles Suit with Messaging App Over Children’s Data Practices October 11, 2016

On October 3, 2016, the Texas Attorney General [announced](#) a \$30,000 settlement with mobile app developer Juxta Labs, Inc. (“Juxta”) stemming from allegations that the company violated [Texas consumer protection law](#) by engaging in false, deceptive or misleading acts or practices regarding the collection of personal information from children. [Continue Reading...](#)

Department of Defense Finalizes Rule for Cyber Incident Reporting October 7, 2016

On October 4, 2016, the U.S. Department of Defense (“DoD”) finalized its [rule](#) implementing the mandatory cyber incident reporting requirements for defense contractors under 10 U.S.C. §§ 391 and 393 (the “Rule”). The Rule applies to DoD contractors and subcontractors that are targets of any cyber incident with a potential adverse impact on information systems and “covered defense information” on those systems. [Continue Reading...](#)

The Arc of a Data Breach: A 3-Part Series to Make Sure You're Prepared **October 6, 2016**

Episode 3: Lessons Learned

In the [third segment](#) of our 3-part series with Lawline, [Lisa J. Sotto](#), head of our [Global Privacy and Cybersecurity](#) practice at Hunton & Williams LLP, discusses the details of the post-mortem following a data breach and the role of boards of directors before, during and after a breach. "We always want to revisit our incident response plan...and make changes to incorporate the lessons learned from a cyber event," Sotto says. "We seek to ensure senior leadership understands how to prevent these events from happening in the future."

[View the third segment](#) and the [presentation materials](#).

CNIL Provides Update on Compliance Pack Regarding Connected Vehicles **October 5, 2016**

On October 3, 2016, at the Paris Motor Show, the French Data Protection Authority ("CNIL") [reported](#) on the progress of a new compliance pack on connected vehicles. The work was [launched](#) on March 23, 2016, and should be finalized in Spring 2017. [Continue Reading...](#)

CIPL and its GDPR Project Stakeholders Discuss DPOs and Risk under GDPR **October 5, 2016**

In September, the [Centre for Information Policy Leadership](#) ("CIPL") held its second GDPR Workshop in Paris as part of its two-year GDPR Implementation Project. The purpose of the project is to provide a forum for stakeholders to promote EU-wide consistency in implementing the GDPR, encourage forward-thinking and future-proof interpretations of key GDPR provisions, develop and share relevant best practices, and foster a culture of trust and collaboration between regulators and industry. [Continue Reading...](#)

EDPS Issues Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data **October 4, 2016**

On September 23, 2016, the European Data Protection Supervisor (the "EDPS") released [Opinion 8/2016](#) (the "Opinion") on the coherent enforcement of fundamental rights in the age of big data. The Opinion updates the EDPS' [Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data](#), first published in 2014, and provides practical recommendations on how the EU's objectives and standards can be applied holistically across the EU institutions. [Continue Reading...](#)

CISPE Unveils Cloud Providers Code of Conduct **October 4, 2016**

On September 27, 2016, Cloud Infrastructure Services Providers in Europe ("CISPE") published its [Data Protection Code of Conduct](#) (the "Code"). CISPE, a relatively new coalition of more than 20 cloud infrastructure providers with operations in Europe, has focused the Code on transparency and compliance with EU data protection laws. [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.