**December 2014**

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:

- German DPA Imposes 1.3 Million EUR Fine on Insurance Group for Violation of Data Protection Law
- FTC Warns Foreign-Based App Developer of Potential COPPA Violations
- FTC Announces Settlement with T-Mobile in Mobile Cramming Case
- Industry, Privacy Advocates Join Microsoft to Protect Customer Emails in Foreign Servers
- FinCEN Assesses Penalty Against Former MoneyGram Compliance Officer
- EU and U.S. Privacy Experts Meet to Develop Transatlantic Privacy "Bridges"
- NLRB Reverses Register Guard; Grants Workers Right to Use Employer Email System for Section 7 Purposes
- Centre for Information Policy Leadership Discusses Privacy Risk Management at the OECD Working Party on Security and Privacy in the Digital Economy
- Centre for Information Policy Leadership Points to New ISO Cloud Privacy Standard as "Accountability" Milestone
- In a Surprising Move, Congress Passes Four Cybersecurity Bills
- CJEU Adopts a Strict Approach to the Use of CCTV
- HHS Reaches Settlement with Health Care Company Over Malware Breach
- Privacy Authorities Call on App Marketplaces to Require Privacy Policies
- New York Banking Regulator Announces New Cybersecurity Assessment Process
- Article 29 Working Party Issues Joint Statement on European Values and Actions for an Ethical European Data Protection Framework
- Article 29 Working Party Publishes Working Document on Surveillance
- NIST Releases Update on Implementation of Cybersecurity Framework
- Centre for Information Policy Leadership Publishes White Paper on "The Role of Risk in Data Protection"
- Article 29 Working Party Issues Working Document Proposing Cooperation Procedure for Issuing Common Opinions on Contractual Clauses
- Asia Pacific Privacy Authorities Hold 42nd Forum in Vancouver to Discuss Hot Global Privacy Topics
- Centre Discusses the Risk-Based Approach to Privacy and APEC-EU Interoperability at IAPP Brussels
- Article 29 Working Party Issues Opinion on Device Fingerprinting
- Poland Amends Its Personal Data Protection Act
- European Parliament Announces New European Data Protection Supervisor

**German DPA Imposes 1.3 Million EUR Fine on Insurance Group for Violation of Data Protection Law**
**December 30, 2014**

On December 29, 2014, the Commissioner for Data Protection and Freedom of Information of the German state Rhineland-Palatinate issued a press release stating that it imposed a fine of €1,300,000 on the insurance group Debeka. According to the Commissioner, Debeka was fined due to its lack of internal controls and its violations of data protection law. Debeka sales representatives allegedly bribed public sector employees during the eighties and nineties to obtain address data of employees who were on path to become civil servants. Debeka purportedly wanted this address data to market insurance contracts to these employees. The Commissioner asserted that the action against Debeka is intended to emphasize that companies must handle personal data in a compliant manner. The fine was accepted by Debeka to avoid lengthy court proceedings. Continue reading…

**FTC Warns Foreign-Based App Developer of Potential COPPA Violations**
**December 23, 2014**

On December 22, 2014, the Federal Trade Commission announced that it notified China-based BabyBus (Fujian) Network Technology Co., Ltd., ("BabyBus") that several of the company's mobile applications ("apps") appear to be in violation of the Children's Online Privacy Protection Rule (the "COPPA Rule"). In a letter dated December 17, 2014, the FTC warned BabyBus of potential COPPA violations stemming from allegations that the company has failed to obtain verifiable parental consent prior to its apps collecting and disclosing the precise geolocation information of users under the age of 13. Continue reading…

**FTC Announces Settlement with T-Mobile in Mobile Cramming Case**
**December 22, 2014**

On December 19, 2014, the Federal Trade Commission announced a settlement of at least $90 million with mobile phone carrier T-Mobile USA, Inc. ("T-Mobile") stemming from allegations related to mobile cramming. This settlement amount will primarily be used to provide refunds to affected customers who were charged by T-Mobile for unauthorized third-party charges. As part of the settlement, T-Mobile also will pay $18 million in fines and penalties to the attorneys general of all 50 states and the District of Columbia, and $4.5 million to the Federal Communications Commission. Continue reading…

**Industry, Privacy Advocates Join Microsoft to Protect Customer Emails in Foreign Servers**
**December 22, 2014**

On December 15, 2014, Microsoft reported the filing of 10 *amicus* briefs in the 2nd Circuit Court of Appeals signed by 28 leading technology and media companies, 35 leading computer scientists, and 23 trade associations and advocacy organizations, in support of Microsoft's litigation to resist a U.S. Government's search warrant purporting to compel the production of Microsoft customer emails that are stored in Ireland. In opposing the Government's assertion of extraterritorial jurisdiction in this case, Microsoft and its supporters have argued that their stance seeks to promote privacy and trust in cross-border commerce and advance a "broad policy issue" that is "fundamental to the future of global technology." Continue reading…

**FinCEN Assesses Penalty Against Former MoneyGram Compliance Officer**
**December 22, 2014**

On December 18, 2014, the Financial Crimes Enforcement Network ("FinCEN") issued a $1 million civil penalty against Thomas E. Haider, the former Chief Compliance Officer of MoneyGram International, Inc. ("MoneyGram"). In a press release announcing the assessment, FinCEN alleged that during Haider's oversight of compliance for MoneyGram, he failed to adequately respond to thousands of customer complaints regarding schemes that utilized MoneyGram to defraud consumers. In coordination with FinCEN, the U.S. Attorney's office in the Southern District of New York filed a civil complaint on the same day, seeking a $1 million civil judgment against Haider to collect on the assessment and requesting injunctive relief barring him from participating in the affairs of any financial institution located or conducting business in the United States. Continue reading…

**EU and U.S. Privacy Experts Meet to Develop Transatlantic Privacy "Bridges"**
**December 19, 2014**

On December 14, 2014, the University of Amsterdam and the Massachusetts Institute of Technology issued a press release about two recent meetings of the EU-U.S. Privacy Bridges Project in Washington, D.C. (held September 22-23, 2014) and Brussels (held December 9-10, 2014). The Privacy Bridges Project is a group of approximately 20 privacy experts from the EU and U.S. convened by Jacob Kohnstamm, Chairman of the Dutch Data Protection Authority and former Chairman of the Article 29 Working Party, to develop practical solutions for bridging the gap between EU and U.S. privacy regimes and legal systems. Bojana Bellamy, President of the Centre for Information Policy Leadership at Hunton & Williams (the "Centre"), and Fred Cate, the Centre's Senior Policy Advisor are members of this group. Continue reading…

**NLRB Reverses Register Guard; Grants Workers Right to Use Employer Email System for Section 7 Purposes**
**December 17, 2014**

As reported in the Hunton Employment & Labor Perspectives Blog:

In Purple Communications, Inc., a divided National Labor Relations Board ("NLRB") held that employees have the right to use their employers' email systems for statutorily protected communications, including self-organization and other terms and conditions of employment, during non-working time. In making this determination, the NLRB reversed its divided 2007 decision in *Register Guard*, which held that employees have no statutory right to use their employer's email systems for Section 7 purposes. Continue reading…

**Centre for Information Policy Leadership Discusses Privacy Risk Management at the OECD Working Party on Security and Privacy in the Digital Economy**
**December 16, 2014**

Former UK Information Commissioner and Centre for Information Policy Leadership (the "Centre") Global Strategy Advisor Richard Thomas was invited to make a presentation at a roundtable on Privacy Risk Management and Next Steps at the Organization for Economic Cooperation and Development's ("OECD's") 37th meeting of the Working Party on Security and Privacy in the Digital Economy ("Working Party"). The meeting was attended by governmental and regulatory officials from most OECD member countries, with various other participants and observers. Continue reading…

**Centre for Information Policy Leadership Points to New ISO Cloud Privacy Standard as "Accountability" Milestone**
**December 15, 2014**

In an article entitled The Rise of Accountability from Policy to Practice and Into the Cloud published by the International Association of Privacy Professionals, Bojana Bellamy, President of the Centre for Information Policy Leadership at Hunton & Williams (the "Centre"), outlines the rapid global uptake of "accountability" as a cornerstone of effective data protection and points to the recent ISO 27018 data privacy cloud standard as one of the latest examples. Continue reading…

**In a Surprising Move, Congress Passes Four Cybersecurity Bills**
**December 12, 2014**

In a flurry of activity on cybersecurity in the waning days of the 113th Congress, Congress unexpectedly approved, largely without debate and by voice vote, four cybersecurity bills that: (1) clarify the role of the Department of Homeland Security ("DHS") in private-sector information sharing, (2) codify the National Institute of Standards and Technology's ("NIST") cybersecurity framework, (3) reform oversight of federal information systems, and (4) enhance the cybersecurity workforce. The President is expected to sign all four bills. The approved legislation is somewhat limited as it largely codifies agency activity already underway. With many observers expecting little legislative activity on cybersecurity before the end of the year, however, that Congress has passed and sent major cybersecurity legislation to the White House for the first time in 12 years may signal Congress' intent to address systems protection issues more thoroughly in the next Congress. Continue reading…

**CJEU Adopts a Strict Approach to the Use of CCTV**
**December 12, 2014**

On December 11, 2014, in response to a request for a preliminary ruling from the Supreme Administrative Court of the Czech Republic, the Court of Justice of the European Union ("CJEU") ruled that the use of CCTV in the EU should be strictly limited, and that the exemption for "personal or household activity" does not permit the use of a home CCTV camera that also films any public space. Continue reading…

**HHS Reaches Settlement with Health Care Company Over Malware Breach**
**December 12, 2014**

The Department of Health and Human Services ("HHS") recently announced a resolution agreement and $150,000 settlement with Anchorage Community Mental Health Services, Inc. ("ACHMS") in connection with a data breach caused by malware. ACHMS, which provides nonprofit behavioral health care services in Alaska, experienced a breach in March 2012 that affected the electronic protected health information ("ePHI") of 2,743 individuals. After ACHMS reported the breach to the HHS Office for Civil Rights ("OCR"), OCR investigated ACHMS and found several HIPAA Security Rule violations, including that ACHMS had failed to: Continue reading…

**Privacy Authorities Call on App Marketplaces to Require Privacy Policies**
**December 12, 2014**

On December 9, 2014, a coalition of 23 global privacy authorities sent a letter to the operators of mobile application ("app") marketplaces urging them to require privacy policies for all apps that collect personal information. Although the letter was addressed to seven specific app marketplaces, the letter notes that it is intended to apply to all companies that operate app marketplaces. Continue reading…

**New York Banking Regulator Announces New Cybersecurity Assessment Process**
**December 11, 2014**

On December 10, 2014, the New York State Department of Financial Services (the "Department") announced that it issued an industry guidance letter to all Department-regulated banking institutions that formally introduces the Department's new cybersecurity preparedness assessment process. The letter announces the Department's plans to expand its information technology examination procedures to increase focus on cybersecurity, which will become a regular, ongoing part of the Department's bank examination process. Continue reading…

**Article 29 Working Party Issues Joint Statement on European Values and Actions for an Ethical European Data Protection Framework**
**December 10, 2014**

On December 8, 2014, the Article 29 Working Party (the " Working Party") and the French Data Protection Authority (the "CNIL") organized the European Data Governance Forum, an international conference centered around the theme of privacy, innovation and surveillance in Europe. The conference concluded with the presentation of a Joint Statement adopted by the Working Party during its plenary meeting on November 25, 2014. Continue reading…

**Article 29 Working Party Publishes Working Document on Surveillance**
**December 10, 2014**

On December 5, 2014, the Article 29 Working Party (the "Working Party") published a Working Document on surveillance, electronic communications and national security. The Working Party (which is comprised of the national data protection authorities ("DPAs") of each of the 28 EU Member States) regularly publishes guidance on the application and interpretation of EU data protection law. Although its views are not legally binding, they are strongly indicative of the way in which EU data protection law is likely to be enforced. Continue reading…

**NIST Releases Update on Implementation of Cybersecurity Framework**
**December 9, 2014**

On December 5, 2014, the National Institute of Standards and Technology ("NIST") released an update on the implementation of the Framework for Improving Critical Infrastructure Cybersecurity ("Framework"). NIST issued the Framework earlier this year in February 2014 at the direction of President Obama's February 2013 Critical Infrastructure Executive Order. The update is based on feedback NIST received in October at the 6th Cybersecurity Framework Workshop as well as from responses to an August Request for Information. Continue reading…

**Centre for Information Policy Leadership Publishes White Paper on "The Role of Risk in Data Protection"**
**December 9, 2014**

The Centre for Information Policy Leadership at Hunton & Williams (the "Centre") has published a second white paper in its multi-year Privacy Risk Framework Project entitled The Role of Risk in Data Protection. This paper follows the earlier white paper from June 2014 entitled A Risk-based Approach to Privacy: Improving Effectiveness in Practice. Continue reading…

**Article 29 Working Party Issues Working Document Proposing Cooperation Procedure for Issuing Common Opinions on Contractual Clauses**
**December 5, 2014**

On November 26, 2014, the Article 29 Working Party (the "Working Party") released a Working Document providing a cooperation procedure for issuing common opinions on whether "contractual clauses" comply with the European Commission's Model Clauses (the "Working Document"). Continue reading…

**Asia Pacific Privacy Authorities Hold 42nd Forum in Vancouver to Discuss Hot Global Privacy Topics**
**December 4, 2014**

On December 2-4, 2014, Asia Pacific Privacy Authority ("APPA") members and invited observers and guest speakers from government, the private sector, academia and civil society met in Vancouver, Canada, to discuss privacy laws and policy issues. At the end of the open session (or "broader session") on day two, APPA issued its customary communiqué ("Communiqué") containing the highlights of the discussions during both the closed session on day one and the open session on day two. A side event on Big Data will be held on the morning of day three (December 4). Continue reading…

**Centre Discusses the Risk-Based Approach to Privacy and APEC-EU Interoperability at IAPP Brussels**
**December 3, 2014**

At the International Association of Privacy Professionals' ("IAPP's") recent Europe Data Protection Congress in Brussels, the Centre for Information Policy Leadership at Hunton & Williams (the "Centre") led two panels on the risk-based approach to privacy as a tool for implementing existing privacy principles more effectively and on codes of conduct as a means for creating interoperability between different privacy regimes. Continue reading…

**Article 29 Working Party Issues Opinion on Device Fingerprinting**
**December 2, 2014**

On November 25, 2014, the Article 29 Working Party (the "Working Party") adopted Opinion 9/2014 (the "Opinion") on device fingerprinting. The Opinion addresses the applicability of the consent requirement in Article 5.3 of the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) to device fingerprinting. As more and more website providers suggest using device fingerprinting instead of cookies for the purpose of providing analytics or for tracking purposes, the Working Party clarifies how the rules regarding user consent to cookies apply to device fingerprinting. Thus, the Opinion expands on Opinion 04/2012 on the Cookie Consent Exemption. Continue reading…

**Poland Amends Its Personal Data Protection Act**
**December 2, 2014**

On November 24, 2014, the Polish President Bronisław Komorowski signed into law a bill that was passed byPolish Parliament on November 7, 2014, which amends, among other laws, certain provisions of the Personal Data Protection Act 1997. As a result of the amendments, data controllers will be able to transfer personal data to jurisdictions that do not provide an "adequate level" of data protection without obtaining the prior approval of the Polish Data Protection Authority (*Generalny Inspektor Ochrony Danych Osbowych* or "GIODO"), provided that they meet certain requirements specified under the bill. In addition, the bill amends Polish law so that it is no longer mandatory to appoint an administrator of information security (*administrator bezpieczeństwa informacji*or "ABI"). An ABI is similar to a data protection officer but an ABI has narrower responsibilities that predominantly concern data security. Continue reading…

**European Parliament Announces New European Data Protection Supervisor**
**December 1, 2014**

On November 27, 2014, the European Parliament announced that it will appoint Giovanni Buttarelli as the new European Data Protection Supervisor ("EDPS"), and Wojciech Wiewiórowski as the Assistant Supervisor. The announcement has been expected since the Parliament's Committee on Civil Liberties, Justice and Home Affairs voted on October 20, 2014 for Buttarelli and Wiewiórowski to be the Parliament's leading candidates for the two positions. The final step of the process is for the Parliament and the Council of the European Union to jointly sign a nomination decision, after which Buttarelli and Wiewiórowski will formally take up their new roles. Continue reading…

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