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

April 2015

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:

- HHS Reaches Settlement with Pharmacy Over Disposal Issues
- Sotto Named Among National Law Journal's "Outstanding Women Lawyers"
- ICO Publishes Summary of Responses to its Big Data Report
- Data Security Act Introduced in New York State Assembly
- Privacy Group Requests D.C. Circuit Review Regarding Lack of Privacy Rules in the FAA's Proposed Drone Regulations
- House of Representatives Passes Two Cybersecurity Bills
- FTC Reaches Settlement in First Enforcement Action Against a Retail Tracking Company
- FCC Joins Asia Pacific Privacy Forum
- Data Localization in a Chinese Context
- French Data Protection Authority Unveils 2014 Annual Activity Report
- Washington State Senate Approves Amendment to Data Breach Notification Law
- UN Human Rights Council Establishes Special Rapporteur on the Right to Privacy
- FTC Announces Settlements with Debt Brokers Who Posted Consumers' Information Online
- FTC Proposes Settlement with Two Companies Over False Safe Harbor Certification Claims
- AT&T Enters into Largest Data Breach Settlement with FCC to Date
- Video: In Depth – Sotto Details Who, What, Why of Today's Cyber Threat Landscape
- UK Court Ruling Allows Claims Against Google for Misuse of Private Information
- GPEN Releases First Annual Report
- President Obama Issues Executive Order Enabling Treasury to Impose Sanctions on Cyber-Enabled Activities

---

HHS Reaches Settlement with Pharmacy Over Disposal Issues
April 30, 2015

The Department of Health and Human Services ("HHS") recently announced a resolution agreement and $125,000 settlement with Cornell Prescription Pharmacy ("Cornell") in connection with the disposal of prescription records in an unsecured dumpster on Cornell's premises. After receiving a report from a Denver television station regarding Cornell's disposal practices, the HHS' Office for Civil Rights ("OCR") investigated Cornell and found several HIPAA Privacy Rule violations, including that Cornell had failed to:

Continue reading…

Sotto Named Among National Law Journal's "Outstanding Women Lawyers"
April 30, 2015

Hunton & Williams LLP announces Lisa J. Sotto, head of the firm's Global Privacy and Cybersecurity practice and managing partner of the New York office, has been named to *The National Law Journal's* "Outstanding Women Lawyers" list. The listing, composed of 75 of the most accomplished female lawyers today, includes women who have surpassed their peers based on their excellence in professional practice, development of new areas of law, leadership roles and influence. Continue reading…

ICO Publishes Summary of Responses to its Big Data Report
April 27, 2015

On April 10, 2015, the UK Information Commissioner's Office ("ICO") published a summary of the feedback received from its July 28, 2014 report on *Big Data and Data Protection* (the "Report"). The ICO plans to revise its Report in light of the feedback received on three key questions and re-issue the Report in the summer of 2015. Below are key highlights set forth in the summary, entitled Summary of feedback on *Big Data and data protection* and ICO response ("Summary of Feedback"). Continue reading…

Data Security Act Introduced in New York State Assembly
April 24, 2015

On April 8, 2015, a New York Assemblyman introduced the Data Security Act in the New York State Assembly that would require New York businesses to implement and maintain information security safeguards. The requirements would apply to "private information," which is defined as either:

- personal information consisting of any information in combination with one or more of the following data elements, when either the personal information or the data element is not encrypted: Social Security number; driver's license number or non-driver identification card number; financial account or credit or debit card number in combination with any required security code or password; or biometric information;
- a user name or email address in combination with a password or security question and answer that would permit access to an online account; or
- unsecured protected health information (as that term is defined in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule).

Continue reading…

Privacy Group Requests D.C. Circuit Review Regarding Lack of Privacy Rules in the FAA's Proposed Drone Regulations
April 24, 2015

On March 31, 2015, the Electronic Privacy Information Center ("EPIC") filed a petition (the "Petition") with the U.S. Court of Appeals for the District of Columbia Circuit accusing the Department of Transportation's Federal Aviation Administration ("FAA") of unlawfully failing to include privacy rules in the FAA's proposed framework of regulations for unmanned aircraft systems ("UAS"), otherwise known as drones. The Petition stems from the FAA's November 2014 denial of another EPIC petition calling for the FAA to address the threat of privacy and civil liberties associated with the deployment of aerial drones within the U.S. Continue reading…

House of Representatives Passes Two Cybersecurity Bills
April 23, 2015

The House of Representatives passed two complimentary bills related to cybersecurity, the "Protecting Cyber Networks Act" (H.R. 1560) and the "National Cybersecurity Protection Advancement Act of 2015" (H.R. 1731). These bills provide, among other things, liability protection for (1) the use of monitoring and defensive measures to protect information systems, and (2) the sharing of cybersecurity threat information amongst non-federal entities and with the federal government. With the Senate having just recently overcome disagreement on sex trafficking legislation and the Attorney General nomination, that body is now expected to consider similar information sharing legislation entitled the "Cybersecurity

Information Sharing Act" (S. 754) in the coming weeks. Assuming S. 754 also is passed by the Senate, the two Chambers of Congress will convene a Conference Committee to draft a single piece of legislation which will be then voted on by the House and Senate, before heading to the President's desk. The White House has not committed to signing any resulting legislation, but has signaled some positive support. Continue reading…

FTC Reaches Settlement in First Enforcement Action Against a Retail Tracking Company
April 23, 2015

On April 23, 2015, the Federal Trade Commission ("FTC") announced that Nomi Technologies ("Nomi") has agreed to settle charges stemming from allegations that the company misled consumers with respect to their ability to opt out of the company's mobile device tracking service at retail locations. The settlement marks the FTC's first Section 5 enforcement action against a company that provides tracking services at retailers. Continue reading…

FCC Joins Asia Pacific Privacy Forum
April 22, 2015

On April 15, 2015, the Federal Communications Commission ("FCC") announced that it has joined the Asia Pacific Privacy Authorities ("APPA"), the principal forum for privacy authorities in the Asia-Pacific Region. APPA members meet twice a year to discuss recent developments, issues of common interest and cooperation. The FCC now joins the Federal Trade Commission as the U.S. representatives to APPA. Continue reading…

Data Localization in a Chinese Context
April 22, 2015

Data localization has been a matter of widespread concern in recent weeks. In an article published in the International Association of Privacy Professionals' *Privacy Perspectives*, Hunton & Williams partner Manuel Maisog explains why lessons from China's past show that its future should have little room for data localization. Maisog states that "[w]hile data localization has most recently and dramatically come to prominence in the form of Russian data localization legislation," it currently "is a global issue." He continues to say that "the Internet has linked the world's information platforms so seamlessly that the effects of a successful data localization effort in any one major country or economy would make itself felt globally and immediately." Continue reading…

French Data Protection Authority Unveils 2014 Annual Activity Report
April 20, 2015

On April 16, 2015, the French Data Protection Authority (the "CNIL") published its Annual Activity Report for 2014 (the "Report") highlighting its main accomplishments in 2014 and outlining some of the topics it will consider further in 2015. Continue reading…

Washington State Senate Approves Amendment to Data Breach Notification Law
April 15, 2015

On April 13, 2015, the Senate of Washington State unanimously passed legislation strengthening the state's data breach law. The bill (HB 1078) passed the Senate by a 47-0 vote, and as we previously reported, passed the House by a 97-0 vote. Continue reading…

UN Human Rights Council Establishes Special Rapporteur on the Right to Privacy
April 14, 2015

On March 26, 2015 the United Nations Human Rights Council (the "Council") announced that it will appoint a new position as special rapporteur on the right to privacy for a term of three years. The position, which is part of the Council's resolution, is intended to reaffirm the right to privacy and the right to the protection of the law against any interference on a person's privacy, family, home or correspondences, as set out in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. Continue reading…

FTC Announces Settlements with Debt Brokers Who Posted Consumers' Information Online
April 14, 2015

On April 13, 2015, the Federal Trade Commission announced that it has settled charges with two debt brokers who posted consumers' unencrypted personal information on a public website. The settlements with Cornerstone and Company, LLC("Cornerstone"), Bayview Solutions, LLC ("Bayview"), and the companies' individual owners resulted from initial complaints about the debt brokers in 2014. Cornerstone and Bayview allegedly had posted the personal information of their debtors in unencrypted Excel spreadsheets on a publicly accessible website geared to buyers and sellers of consumer debt. The information included consumers' names, addresses, credit card numbers, bank account numbers and debt amounts. Continue reading…

FTC Proposes Settlement with Two Companies Over False Safe Harbor Certification Claims
April 13, 2015

On April 7, 2015, the FTC announced proposed settlements with TES Franchising, LLC, an organization specializing in business coaching, and American International Mailing, Inc., an alternative mail transporting company, related to charges that the companies falsely claimed they were compliant with the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks. Continue reading…

AT&T Enters into Largest Data Breach Settlement with FCC to Date
April 8, 2015

On April 8, 2015, the Federal Communications Commission announced a $25 million settlement with AT&T Services, Inc. ("AT&T") stemming from allegations that AT&T failed to protect the confidentiality of consumers' personal information, resulting in data breaches at AT&T call centers in Mexico, Colombia and the Philippines. The breaches, which took place over 168 days from November 2013 to April 2014, involved unauthorized access to customers' names, full or partial Social Security numbers and certain protected account-related data, affecting almost 280,000 U.S. customers. Continue reading…

Video: In Depth – Sotto Details Who, What, Why of Today's Cyber Threat Landscape
April 6, 2015

From Wall Street to Main Street to Hollywood, steering clear of a data breach is challenging in a world where it is no longer a question of *if* but rather a matter of *when* your company will be hit. Hunton & Williams' Chair of the Global Privacy and Cybersecurity practice Lisa Sotto speaks in depth with associate Brittany Bacon about three groups of attackers, how they are infiltrating IT systems, what they are looking for, and how you can prepare. Today, Sotto says, cybersecurity is a legal issue, a risk issue and a governance issue, and one that matters to shareholders, boards of directors and regulators.

View the video segment.

UK Court Ruling Allows Claims Against Google for Misuse of Private Information
April 2, 2015

On March 27, 2015, the England and Wales Court of Appeal issued its judgment in *Google Inc. v Vidal-Hall and Others*. Google Inc. ("Google") appealed an earlier decision by Tugendhat J. in the High Court in January 2014. The claimants were users of Apple's Safari browser who argued that during certain months in 2011 and 2012, Google collected information about their browsing habits via cookies placed on their devices without their consent and in breach of Google's privacy policy. Continue reading…

GPEN Releases First Annual Report
April 2, 2015

On April 1, 2015, the Global Privacy Enforcement Network ("GPEN") released its 2014 annual report (the "Report"). This Report marks the first time that GPEN has issued an annual report highlighting the network's accomplishments throughout the year. GPEN is a network of approximately 50 privacy enforcement authorities from around the world, including the Federal Trade Commission and the Federal Communications Commission. Continue reading…

President Obama Issues Executive Order Enabling Treasury to Impose Sanctions on Cyber-Enabled Activities
April 1, 2015

As reported in *Bloomberg BNA*, on April 1, 2015, the White House announced that President Obama has signed a new executive order providing the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, the ability to impose sanctions on individuals and entities that engage in certain cyber-enabled activities. The signed executive order, entitled Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (the "Executive Order"), focuses on blocking the property or interests in property located in the United States of persons engaging in cyber-enabled activities that cause a significant threat to the national security, foreign policy, economic health or financial stability of the U.S. (collectively, the "Significant Threat"). 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.