

PRIVACY & INFORMATION SECURITY LAW BLOG

Global Privacy and Cybersecurity Law Updates and Analysis



September 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:

- [CJEU Announces Date for Judgment on Safe Harbor](#)
- [Blockchain, Cybersecurity and Global Finance](#)
- [Seventh Circuit Denies En Banc Review For Data Breach Class Action](#)
- [SEC Announces Settlement Order and Publishes Investor Alert](#)
- [U.S.-EU Data Transfer Agreement for Law Enforcement Nearing Completion](#)
- [Advocate General of the European Court of Justice Issues Opinion Regarding Safe Harbor](#)
- [Target Data Breach Litigation: District Court Certifies Class of Financial Institutions](#)
- [SEC Issues Top Cybersecurity Priorities for Broker-Dealers and Investment Advisers](#)
- [German DPA Fines Data Controller for Inadequate Data Processing Agreement](#)
- [ICO to Investigate Data Sharing for Marketing by UK Charities](#)
- [APEC Privacy Recognition for Processors Ready for Implementation](#)
- [CNIL Publishes Internet Sweep Results and New Guidelines for Websites Aimed at Children](#)
- [Department of Defense Issues New Cyber Incident Reporting and Cloud Computing Requirements for Contractors](#)
- [German Data Protection Commissioners Issue Position Paper on Proposed EU General Data Protection Regulation](#)

CJEU Announces Date for Judgment on Safe Harbor September 30, 2015

On September 29, 2015, the Court of Justice of the European Union ("CJEU") [announced](#) that it will deliver its judgment in the [Schrems vs. Facebook](#) case on October 6, 2015. The CJEU's judgment will be the final ruling in the case, and comes after the Advocate General's [Opinion](#) regarding Safe Harbor earlier this week. [Continue reading...](#)

Blockchain, Cybersecurity and Global Finance September 30, 2015

When novelist William Gibson said, "[t]he future is already here, it's just not very evenly distributed," he may have had innovation like blockchain technology in mind. In the near future, blockchain may become the new architecture of a reinvented global financial services infrastructure. The technology – a distributed, consensus-driven ledger that enables and records encrypted digital asset transfers without the need of a confirming third party – is revolutionary to global financial services, whose core functions include the trusted intermediary role (e.g., payment processor, broker, dealer, custodian). [Continue reading...](#)

Seventh Circuit Denies En Banc Review For Data Breach Class Action September 29, 2015

On September 17, 2015, the Seventh Circuit [rejected](#) Neiman Marcus' petition for a rehearing *en banc* of [Remijas v. Neiman Marcus Group, LLC, No. 14-3122](#). In *Remijas*, a Seventh Circuit panel found that

members of a putative class alleged sufficient facts to establish standing to sue Neiman Marcus following a 2013 data breach that resulted in hackers gaining access to customers' credit and debit card information. No judge in regular active service requested a vote on the rehearing petition. Additionally, all members of the original panel voted to deny rehearing. As we [previously reported](#), and according to [The Practitioner's Handbook for Appeals to the United States Court of Appeals for the Seventh Circuit](#), "it is more likely to have a petition for writ of certiorari granted by the Supreme Court than to have a request for *en banc* consideration granted" in the Seventh Circuit. [Continue reading...](#)

SEC Announces Settlement Order and Publishes Investor Alert September 25, 2015

On September 22, 2015, the Securities and Exchange Commission ("SEC") [announced](#) a [settlement order](#) (the "Order") with an investment adviser for failing to establish cybersecurity policies and procedures, and published an investor alert (the "Alert") entitled [Identity Theft, Data Breaches, and Your Investment Accounts](#). [Continue reading...](#)

U.S.-EU Data Transfer Agreement for Law Enforcement Nearing Completion September 24, 2015

On September 8, 2015, representatives from the U.S. Government and the European Commission initialed a draft agreement known as the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses (the "Umbrella Agreement"). The European Commission's [stated aim](#) for the Umbrella Agreement is to put in place "a comprehensive high-level data protection framework for EU-U.S. law enforcement cooperation." The Umbrella Agreement has been agreed upon amid the ongoing uncertainty over the future of the U.S.-EU Safe Harbor, and was drafted shortly before the release of the September 23 [Advocate General's Opinion](#) in the [Schrems v. Facebook](#) litigation. The content of the Umbrella Agreement is in its final form, but its implementation is dependent upon revisions to U.S. law that are currently before Congress. [Continue reading...](#)

Advocate General of the European Court of Justice Issues Opinion Regarding Safe Harbor September 23, 2015

On September 23, 2015, Advocate General of the European Court of Justice Yves Bot issued his [Opinion](#) in the case of [Max Schrems](#), which is currently pending before the Court of Justice of the European Union (the "CJEU"). In the opinion, the Advocate General provided his views concerning two key issues related to the U.S.-EU Safe Harbor Framework: (1) the powers of national data protection authorities to investigate and suspend international data transfers made under the Safe Harbor Framework and (2) the ongoing validity of the European Commission's Safe Harbor adequacy decision (Decision 2000/520). [Continue reading...](#)

Target Data Breach Litigation: District Court Certifies Class of Financial Institutions September 23, 2015

On September 15, 2015, Judge Magnuson of the U.S. District Court for the District of Minnesota [certified](#) a Federal Rule of Civil Procedure 23(b)(3) class of financial services institutions claiming damages from Target Corporation's 2013 data breach. The class consists of "all entities in the United States and its Territories that issued payment cards compromised in the payment card data breach that was publicly disclosed by Target on December 19, 2013." [Continue reading...](#)

SEC Issues Top Cybersecurity Priorities for Broker-Dealers and Investment Advisers September 22, 2015

On September 15, 2015, the Office of Compliance, Inspections and Examinations (“OCIE”) at the U.S. Securities and Exchange Commission (“SEC”) [issued](#) a Risk Alert outlining its latest cybersecurity examination priorities for SEC-registered broker-dealers and investment advisers. [Continue reading...](#)

German DPA Fines Data Controller for Inadequate Data Processing Agreement September 17, 2015

On August 20, 2015, the Bavarian Data Protection Authority (“DPA”) issued a [press release](#) stating that it imposed a significant fine on a data controller for failing to adequately specify the security controls protecting personal data in a data processing agreement with a data processor. [Continue reading...](#)

ICO to Investigate Data Sharing for Marketing by UK Charities September 16, 2015

On September 2, 2015, the Information Commissioner’s Office (the “ICO”) [announced](#) an investigation into the data sharing practices of charities in the United Kingdom. The announcement follows the publication of an [article](#) in a UK newspaper highlighting the plight of Samuel Rae, an elderly man suffering from dementia. In 1994, Rae completed a survey, which resulted in a charity collecting his personal data. The charity, in turn, allegedly shared his contact details with other charities, data brokers and third parties. Over the years, some of those charities and third parties are reported to have sent Rae hundreds of unwanted items of mail, requesting donations and, in some cases, attempting to defraud him. The legal basis on which Rae’s details were shared remains unclear, although the ICO has noted that the distribution may have resulted from a simple failure to tick an “opt-out” box on the survey. [Continue Reading...](#)

APEC Privacy Recognition for Processors Ready for Implementation September 8, 2015

The APEC Cross-Border Privacy Rules (“CBPR”) system for information controllers received a significant boost during the recent APEC privacy meetings in the Philippines when APEC finalized a corollary certification scheme for information processors, the APEC Privacy Recognition for Processors (“PRP”). As we [previously reported](#), the PRP allows information processors to demonstrate their ability to effectively implement an information controller’s privacy obligations related to the processing of personal information. In addition, the PRP enables information controllers to identify qualified and accountable processors, as well as assist small or medium-sized processors that are not widely known to gain visibility and credibility. Combined, the CBPR for controllers and PRP for processors now covers the entire information ecosystem, promising to motivate additional APEC economies to join both the CBPR and PRP systems, as well as incentivizing larger numbers of controllers and processors to seek certification. [Continue reading...](#)

CNIL Publishes Internet Sweep Results and New Guidelines for Websites Aimed at Children September 3, 2015

On September 2, 2015, the French Data Protection Authority (“CNIL”) [published](#) the results of an Internet sweep of 54 websites visited by children and teenagers. The sweep was conducted in May 2015 to assess whether websites that are directed toward, frequently used by or popular among children comply with French data protection law. As we [previously reported](#), the sweep was coordinated by the Global Privacy Enforcement Network (“GPEN”), a global network of approximately 50 data protection authorities

("DPAs"). The CNIL and 28 other DPAs that are members of the GPEN participated in the coordinated online audit. A total of 1,494 websites and apps were audited around the world. [Continue Reading...](#)

Department of Defense Issues New Cyber Incident Reporting and Cloud Computing Requirements for Contractors
September 3, 2015

On August 26, 2015, the U.S. Department of Defense ("DoD") [published](#) an interim rule entitled Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013–D018) (the "Interim Rule"), that streamlines the obligations for contractors to report network penetrations and establishes DoD requirements for contracting with cloud computing service providers. The Interim Rule amends the information security contracting framework set forth in the Defense Federal Acquisition Regulation Supplement ("DFARS") to implement section 941 of the National Defense Authorization Act ("NDAA") for Fiscal Year ("FY") 2013 and section 1632 of the NDAA for FY 2015, both of which impose cyber incident reporting obligations on contractors. [Continue Reading...](#)

German Data Protection Commissioners Issue Position Paper on Proposed EU General Data Protection Regulation
September 3, 2015

On August 14 and August 26, 2015, the Conference of the Data Protection Commissioners of the Federal Government and the Federal States (Länder) issued a [detailed position paper](#) ("Position Paper") and a [press release](#) on the main issues for the trilogue negotiations on the proposed EU General Data Protection Regulation (the "Regulation"). In the Position Paper and press release, the participating German Data Protection Commissioners ("German DPAs") request the trilogue partners to focus on the following issues. [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.