Welcome
Welcome to the ABA E-Privacy Law Committee's new monthly newsletter.

The ABA E-Privacy Law Committee is a forum for sharing information concerning cutting-edge legal developments with respect to information privacy, both domestically and globally. It provides opportunities for networking with colleagues in the same field, discussing a wide range of privacy issues, commenting on developing practices and guidelines regarding privacy, participating in the development of publications, taking positions on policy issues. The ABA E-Privacy Law Committee features a listserv, offers periodic meetings, teleconferences and publications.

The ABA E-Privacy Law Committee is ramping up its industry participation with a series of new initiatives, including this new monthly publication. Going forward, this newsletter will include brief news statements of current events, links to related sources, and suggested readings.

I hope you enjoy reading our newsletter and if there is anything you would like us to feature in the coming months, then please feel free to contact me.

Paul Lanois
Email: paulanocom@aol.com

E.U. and U.S. Reach Agreement in Principal for SafeHarbor 2.0
European Union and U.S. officials have reached an agreement in principle on a new data transfer agreement following the European Court of Justice’s decision Schrems, which invalidated the Safe Harbor framework. Points of contention between the parties are the U.S.’s failure to maintain safeguards that are equivalent to those found in the EU and U.S. intelligence agencies’ access to E.U. user data. The passage of the USA Freedom Act, issuance of Presidential Policy Directive 28, and establishment of annual joint reviews of the new framework were all critical to the initial negotiations. While parties are
hopeful that these negotiations are a step in the right direction, further talks need to occur before a new framework can be developed and implemented. Representatives from the E.U. and the U.S. have until January 2016 to reach a deal, otherwise EU data protection authorities may undertake coordinated enforcement actions.

On October 16, 2015, an Article 29 Working Party provided guidance on best practices prior to the establishment of the new framework. The Party indicated that data transfers could no longer be based upon the invalidated Safe Harbor Framework, and companies should use Standard Contractual Clauses ("SCCs") and Binding Corporate Rule ("BCRs") in the interim. This guidance has received a mixed response throughout the EU. On October 28, 2015, Germany announced it would not announce new approved data transfers pursuant to BCRs. They also launched investigations into the data transfer practices of several American companies, including Facebook and Google. The Spanish data protection authority sent letters to companies operating in Spain that they should inform it no later than January 29, 2016 of any mechanisms that have been implemented to ensure adequate protections for personal data transferred to the United States. In contrast, Switzerland indicated on October 22, 2015 that companies should rely on “contractual guarantees” as provided by local law, and on October 19, 2015, Israel revoked all transfers relying on the former Framework. Likewise, on October 26, 2015, the Commissioner for Data Protection for the Dubai International Financial Centre (the DIFC) has indicated that data controllers transferring personal data to the US cannot rely any longer on the Safe Harbor schemer and should rely on alternative data transfer mechanisms.

On 6 November, 2015, the European Commission published a communication and a Q&A guidance on the matter. In the communication, the European Commission indicated that its objective is to conclude discussions with the United States in three months. It further indicated that businesses can pursue data transfers to the United States on the basis of contractual solutions and binding corporate rules.

Cloud providers are already taking action. On 6 November 2015, Amazon announced it will build a data center in London by 2017 to ensure “strong data sovereignty to local users”. Microsoft has partnered with Deutsche Telekom to offer cloud services from two new data centers in Germany. The particularity of Microsoft’s announcement is that Deutsche Telekom’s corporate customer unit T-Systems will be acting as a data trustee for
Microsoft's customers' data. Under the contract, Microsoft would have no access to customer data unless granted by T-Systems or customers.

Suggested:


Epic.org: Max Schrems v Irish Data Protection Commissioner (Safe Harbor)

Q&A Guidance from the European Commission

**Consumer Tracking in the Retail Industry**
Retailers’ are exploring new technologies to track and analyze shoppers as they move through retail outlets. [Wal-Mart has tested](https://www.walmart.com/) earlier this year a system that scanned the face of everyone entering certain stores in order to identify suspected shoplifters. It appears that such technology was tested in several stores for a number of months, but the program was then discontinued because of the lack of a return on investment. The use of mobile phone-tracking is however growing in popularity to understand shopper behavior in stores. Such new technologies raise privacy issues. In particular, as pointed out by one of our editors, attorney Paul Lanois, quoted in Forbes, “If enough data can be tied to an identifier over the course of time, then it would be possible of course to identify the user of the device.”

Suggested:

Shopper Phone Tracking: Creepy Spying Or Valid Consumer Research?

Privacy trade-offs in retail tracking

**Facebook faces daily fine in Belgium for tracking non-users**
A Belgian court has ruled that Facebook must stop using cookies to track the online activities of non-Facebook users in Belgium unless they have their explicit consent. Facebook was given 48 hours to comply, or else it would face a daily fine of €250,000. According to media reports, Facebook plans to appeal the decision.

Suggested:
Facebook faces daily fine in Belgium over privacy

FCC Fines Cox Communications over Data Breach

The Federal Communications Commission has entered into a $595,000 settlement with Cox Communications in relation to a data breach in 2014 that exposed customers' personal information to third parties. The settlement also requires Cox to identify all affected customers, notify them of the breach, and provide them one year of free credit monitoring. The FCC indicated that this is its first privacy and data security enforcement action against a cable operator. This ruling could be sign of things to come as data breaches attract more media attention and scrutiny.

Source:

Cox Communications to Pay $595,000 to Settle Data Breach Investigation

Upcoming: On the Leading Edge of Cybersecurity and Privacy Standards

Don’t miss the upcoming program below, co-sponsored by SciTech’s Homeland Security, E-Privacy, Information Security and Technical Standardization committees, Public Contract Law’s Cybersecurity, Privacy and Data Protection Committee, and the Cybersecurity Legal Task Force:

“On the Leading Edge of Cybersecurity and Privacy Standards: Experts from NIST Discuss the Latest Developments and Issues for the Public Sector”

on Monday, December 7, 2015 at 12:00 PM ET, to be presented live in Washington, DC and via teleconference.

For decades, the National Institute of Standards and Technology (NIST) has been at the forefront in developing standards and building consensus for information security and privacy covering an expansive range of topics from defining security and privacy controls to establishing encryption protocols to preparing guidelines for confidentiality of personally identifiable information (PII).

In recent years, NIST’s initiatives have transformed security and privacy standards in both the public and private sectors by harmonizing security and privacy controls for federal agencies and
Contractors (e.g., NIST Special Publication 800-53 Rev. 4), developing the Cybersecurity Framework for use in the private sector, and integrating privacy controls into the security standards.

This panel of NIST experts will address the latest developments in NIST security and privacy standards and discuss what's ahead in emerging security and privacy issues.

Panel
- Naomi Lefkowitz – NIST Senior Privacy Policy Advisor
- Adam Sedgewick – NIST Senior Information Technology Policy Advisor

Moderator
Peter Miller – Senior Counsel, Crowell & Moring LLP; former FTC Chief Privacy Officer; ABA SciTech E-Privacy Co-Chair

Register Today!

More information is available here.

New content contributors
On behalf of our Committee leadership, we are pleased to introduce our new content contributors. Their names and bios are listed below.

HJ Brehmer (hb6732a@student.american.edu) is a 1L at American University’s Washington College of Law. Prior to law school, she founded the E-Crime Investigations team at Yahoo, where she conducted a variety of criminal investigations for referral to law enforcement, domestically and internationally. These cases involved investigations of international hacking rings, large-scale account takeovers, advertising fraud, and individuals possessing and trafficking in CSAI materials. She is interested in both privacy and data security issues, primarily looking at the balance of interests between users, companies, and law enforcement. She graduated from the University of Washington, Seattle in 2012.

Kayla Gardner (kdgardner@law.bison.howard.edu) is a 2L at Howard University School of Law. She holds a Master's Degree in Criminology from GWU. She is active in the Federal Communications Bar Association, the Washington Bar Association, and the Howard Public Interest Law Society. Kayla interned last summer at the FCC in the Bureau of Public Safety and Homeland Security. She currently holds a Fall semester externship at the FCC in Commissioner Clyburn's office. She is originally from Nashville, TN, but has lived in
the DC-metro area for nearly 10 years. She is interested in communications law, especially issues concerning national security and public safety such as data privacy and cybersecurity.

Paul Lanois, LL.M. (paulanocom@aol.com), is an attorney admitted to the New York Bar and the Paris (France) Bar. He regularly publishes articles on technology law and is frequently invited to speak on such topics. He was an Associate Professor at the University of Cergy-Pontoise in France and an associate at major international law firms (Simpson Thacher & Bartlett, Allen & Overy, Linklaters). He is currently senior legal counsel at an international financial institution. He graduated from the University of Paris-Sorbonne (France) with a Master's degree in Business Law and a postgraduate degree in Private and Public Economic Law. He also holds an LL.M. degree from the University of Pennsylvania Law School (USA) and the Wharton Certificate in Business and Public Policy from the Wharton School of the University of Pennsylvania. He holds the CIPP/US, CIPP/E, CIPP/C and CIPT certifications.

Publications Promo Code
SciTech members interested in our product resources may receive 25% on any of our three upcoming cyber webinars and drones book through the end of December. All four are available for 40% off using the following discount code: STCYBER25.


The CLEs are:

Understanding Drone Privacy Law Regarding Unmanned Aerial Vehicles (UAVs);

Structuring Master Service Agreements with First Responders, Forensic Vendors, and E-discovery Providers;

Flying on the Legal Edge with Drones: Emerging Acquisition, Security, and Regulatory Issues for Unmanned Aerial Vehicles