Dear Readers,

Please find below the latest edition of the SciTech E-Privacy Law Committee Newsletter. Please do not hesitate to contact us with any comments, questions, ideas or contributions you may have for this newsletter.

Paul Lanois
Editor
paulanocom@aol.com

LabMD scores win in FTC appeal

A federal court of appeals has granted a temporary "stay," or delay, in implementing the Federal Trade Commission's consent order against LabMD.

The U.S. Court of Appeals for the Eleventh District, in its Nov. 10 ruling listed several reasons for granting the temporary stay. That includes the appellate court's uncertainty about whether the FTC "reasonably interpreted" that the LabMD data security incident at the center of the case was likely to cause significant risk to consumers.

The court wrote "we do not read the word "likely" to include something that has a low likelihood. We do not believe an interpretation that does this is reasonable." The court also found that the costs of complying with the FTC's Order would cause LabMD irreparable harm in light of its current financial situation.

Read more: Gov Info Security - Court Grants LabMD a 'Stay' of FTC Consent Order
See also: LabMD stay opinion (10 Nov 2016)

Russia blocks LinkedIn for violation of local data storage law

LinkedIn has become the first major social networking website to be blocked by the Russian authorities for violating the Russian data storage law. Russian law requires internet companies that process Russian citizens' personal information
to store the user data on servers physically located in Russia. The law came into effect in September 2015.

Read more:
[CNN - Russia has banned LinkedIn](https://www.cnn.com/2016/09/22/technology/russia-linkedin-blockage/)  
[Reuters - Russia starts blocking LinkedIn website after court ruling](https://www.reuters.com/article/us-russia-technology-linkedin-idUSKBN10H1O5)

**Facebook WhatsApp data collection stopped in EU**

Facebook has stopped collecting WhatsApp user data across Europe, the Financial Times reports, bowing to pressure from privacy watchdogs across the continent. The shift in policy means that European users of the messaging app will no longer have information — including phone numbers — relayed to Facebook, but the social network says it may only be a temporary suspension while the laws are debated.

Read more:  
[The Verge - Facebook stops collecting WhatsApp user data in Europe after government pressure](https://www.theverge.com/2016/10/21/13394998/facebook-whatsapp-stop-data-collection-europe)

**Privacy Shield coming under fire, again**

Privacy advocacy group Digital Rights Ireland is challenging the EU-US "Privacy Shield" (allowing for EU-US data transfers based on self-certification by US companies) before the Court of Justice of the European Union (the "CJEU"), accusing it of failing to provide sufficient guarantees to ensure adequate data protection.

Digital Rights Ireland is not the only one going after the Privacy Shield - French privacy advocacy group La Quadrature du Net, non-profit Internet service provider French Data Network, and its Federation FDN industry association have also challenged the adoption of the Privacy Shield before the CJEU.

Privacy advocacy groups are not the only ones looking into the Privacy Shield. Following media reports that Yahoo had scanned all incoming customer emails in 2015 for a digital signature linked to a foreign state sponsor of terrorism, at the behest of a secret court order, the European Commission has asked the United States to provide clarifications on the scope of the court order.

Read more:  
[Reuters - EU questions U.S. over Yahoo email scanning, amid privacy concerns](https://www.reuters.com/article/us-eu-us-privacy-shield/eu-questions-us-over-yahoo-email-scanning-amid-privacy-concerns-idUSKBN1160T5)

**Tesco would face £1.9bn fine under GDPR following hack**
The banking arm of Britain's biggest retailer Tesco faced earlier this month an attack on a number of its customers' accounts, with the theft of about £2.5m from 9,000 accounts. Tesco has confirmed that all customer accounts affected by fraud have been refunded. According to some reports, Tesco would face a fine of over £1.9bn for the hack if it occurred under the EU's GDPR.

The implementation of appropriate cybersecurity measures is getting a lot more attention nowadays, with telecoms company TalkTalk receiving last month a record £400,000 fine by the UK's Information Commissioner's Office for security failings that allowed a cyber attacker to access customer data "with ease".

Read more:
The Inquirer - Tesco Bank hack: Tesco would face £1.9bn fine under GDPR
Information Commissioner's Office - TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack

**IP Addresses are personal data, says CJEU**

On 19 October 2016, the CJEU issued its judgment in *Patrick Breyer v. Bundesrepublik Deutschland*. The CJEU ruled that a dynamic Internet protocol ("IP") address of a website user is personal data, with respect to the website operator, if that operator has the legal means allowing it to identify the user concerned with additional information about that user which is held by an Internet Service Provider ("ISP").

Read more:
Eversheds - Court of Justice of the European Union rules IP addresses are personal data

**UK to implement the EU GDPR despite Brexit**

The UK government has confirmed that the UK will soon be implementing the EU General Data Protection Regulation (the GDPR) despite the Brexit. Following the announcement by the UK's Secretary of State, the Information Commissioner, Elizabeth Denham, has posted a message in which she welcomed the announcement as "good news for the UK" and recognised that the GDPR provides data subjects with greater control over their personal data than the current legislative regime.

Read more:
Information Commissioner's Office - How the ICO will be supporting the implementation of the GDPR

**German DPAs to audit 500 companies on international data transfers**

The German data protection authorities have announced that
they have chosen 500 companies throughout Germany to audit their transfer of personal data to the US and other countries (eg. India). The targets were chosen by random and cover small, medium-size and also large companies known to transfer data of their customers or employees from Germany to the US.

Read more: 
Privacy and Cybersecurity Law - Germany to audit 500 companies

Internet of Things or how a connected toaster may bring down the Internet

The recent massive Internet attack that has recently caused outages and network congestion for a large number of Web sites appears to have been caused with the help of hacked “Internet of Things” (IoT) devices, such as CCTV video cameras and digital video recorders.

If you are interested in reading more about how to protect devices from such security risks, the Cloud Security Alliance (CSA) has released a new detailed and hefty guidance report titled Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products created to help designers and developers of Internet of Things (IoT) related products and services understand the basic security measures that must be incorporated throughout the development process.

Read more: 
Krebs on Security - Hacked Cameras, DVRs Powered Today's Massive Internet Outage
New York Times - A New Era of Internet Attacks Powered by Everyday Devices
Cloud Security Alliance - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products
NIST Internet of Things Cybersecurity Guidance
US Department of Homeland Security - Guidance on Strategic Principles for Securing the Internet of Things

National Law Journal's "Cybersecurity and Data Privacy Trailblazers"

The National Law Journal released the list of its second annual "Cybersecurity and Data Privacy Trailblazers", a group of 50 individuals who made an impact in cybersecurity.

"While those recognized impact the practice of law in different ways, a common thread ties them together: each has shown a deep passion and perseverance in pursuit of their mission, having achieved remarkable successes along the way," according to the National Law Journal.

Read more: 
National Law Journal's Cybersecurity and Data Privacy Trailblazers
Future events

**How to Successfully Train Lawyers and Firm Employees to Safeguard Client Data**

As more states adopt ABA Model Rule 1.6(c) and its mandate to protect client-related information, firms are responding by adopting systems and technology to protect client data. Yet humans are usually identified as the weakest link in data security. Discover how training your firm's lawyers and staff can help protect your clients' data and safeguard it against threats. You will also receive practical tips on improving and testing your security, and in dealing with a breach should one occur.

**Format:** Webinar  
**Date:** November 30, 2016  
**Time:** 01:00 PM - 02:00 PM ET  
**Credits:** 1.00 General CLE Credit Hours  
**Panelist:** Michael P Downey  
**Moderator:** Vaughan W Butts CRISC

[Register here](#) for the webinar.

**U.S. Drone Law: Current Status, Future Direction**

This program brings together a panel of legal practitioners to discuss a breadth of issues related to the use of drones in the United States. The panel will examine the new FAA Part 107 rule and what it means for commercial drone use going forward, including an analysis of the overall requirements, pilot requirements and prohibitions.

In addition to the new FAA rules, the panel will review the proposed "Micro UAS" ARC recommendations for drones under 5 pounds (with a focus on safety issues related to flights over humans), anti-collision laws (TCAS I and II with a special focus on drone considerations), FCC radio communications laws and safety, and practical operations issues related to commercial drone use. Using the new rules and proposed legislation as a foundation, the panel will also address legal issues arising from drone use, including:

- Likely claims
- Hardware and software product liability concerns
- Evidentiary and preemption issues

The panel will round out its discussion by taking a broader look at the ethical and social dimensions of drone security and a forward look at how the law may adapt to address drone use in the future.

**Format:** Webinar  
**Date:** December 7, 2016  
**Time:** 01:00 PM - 02:30 PM ET  
**Credits:** 1.50 General CLE Credit Hours
Panelists: Donna Ann Dulo; Jen Geary; John D Goetz and Yanai Z Siegel
Moderator: Shannon Janel Harmon

Register here for the webinar.