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

News

Illinois Geolocation Privacy Bill's sponsor seeking veto override

Illinois legislation that would require companies to obtain consent before selling customer geolocation data may see new life, with its sponsor telling Bloomberg BNA that she will work to override a recent veto.

Rep. Ann Williams (D) is developing a strategy to try and override the Sept. 22 veto by Gov. Bruce Rauner (R), Carter Harms, Williams’ chief of staff, told Bloomberg BNA. But an override will be difficult.

The Illinois Chamber of Commerce as well as companies including Google, eBay, Expedia, Facebook and Verisign, together with some trade groups representing large tech firms, opposed the legislation.

Read more:
Bloomberg BNA - Illinois Geolocation Privacy Bill Sponsor Seeking Veto Override

Ninth Circuit confirms that a cy pres only settlement can work in a privacy class action

In a recent opinion, the Ninth Circuit upheld a district court’s approval of a class action settlement in a privacy litigation where the class received no damages, and the settlement funds went to cy pres recipients instead. In the
Apple revamps "Privacy" site to promote benefits of privacy technologies

NotPetya ransomware cost FedEx $300 million

Other privacy-related news this month

concerns

In the case In re Google Referrer Header Privacy Litigation, No. 15-15858 (9th Cir. Aug. 22, 2017), the plaintiffs challenged Google’s practice of providing websites with the search terms that individuals used in Google’s search engine to reach the website. The plaintiffs claimed this violated their privacy.

The parties reached a settlement with an $8.5 million fund. Of that, $3.2 million was set aside for attorneys’ fees, administration costs, and incentive payments, the remaining $5.3 million was allocated to six cy pres recipients, and class members received nothing. The Ninth Circuit affirmed the district court’s approval of the settlement, holding that a cy pres only settlement was appropriate where the settlement fund was “non-distributable.”

In the case, there were 129 million class members. If the $5.3 million settlement had been distributed, each class member would have received “a paltry 4 cents.” The court held that, because each class member’s recovery would have been de minimis, a cy pres only settlement was appropriate.

Read more:

In re Google Referrer Header Privacy Litigation, No. 15-15858 (9th Cir. 2017)

The National Law Review - Ninth Circuit Confirms that a Cy Pres Only Settlement Can Work In Privacy Class Action

Inside Counsel - Google Gets 9th Circuit Blessing for $8.5M 'Cy Pres-Only' Deal

Google's email scanning class settlement OK'd on second try

Bloomberg BNA reports that Google has convinced a federal court that changes to a proposed settlement of class claims over scanning user emails are sufficient to now gain preliminary approval (Matera v. Google, Inc., N.D. Cal., No. 15-cv-04062, settlement preliminary approval 8/31/17).

The case highlights the importance of using specific, clear, and detailed language to explain how a defendant will implement technical measures for providing the injunctive relief set out in a settlement. The addition of a few words detailing how Google will implement its promise to not scan and store user email data without consent was enough to convince the court to preliminarily approve a settlement that it had previously rejected.

Read more:

Bloomberg BNA - Google Email Scanning Class Settlement OK'd on Second Try
Companies settle FTC charges relating to false participation in EU-US Privacy Shield framework

Three U.S. companies have agreed to settle Federal Trade Commission charges that they misled consumers about their participation in the European Union-United States Privacy Shield framework, which allows companies to transfer consumer data from EU member states to the United States in compliance with EU law.

In separate complaints, the FTC alleges that human resources software company Decusoft, LLC, printing services company Tru Communication, Inc. (doing business as TCPrinting.net), and Md7, LLC, which manages real estate leases for wireless companies, violated the FTC Act by falsely claiming that they were certified to participate in the EU-US Privacy Shield.

The FTC also alleged that Decusoft falsely claimed participation in the Swiss-U.S. Privacy Shield framework. Despite these claims, all three companies failed to complete the certification process for the Privacy Shield, according to the FTC complaints.

"Today’s actions highlight the FTC’s commitment to aggressively enforce the Privacy Shield frameworks, which are important tools in enabling transatlantic commerce,” said Acting FTC Chairman Maureen K. Ohlhausen. “Companies that want to benefit from these agreements must keep their promises or we will hold them accountable.”

Read more:

US Federal Trade Commission - Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework

EU – US Privacy Shield: Commissioner Jourová wraps up the meetings with US administration on the annual review

Commissioner for Justice, Consumers and Gender Equality, Vera Jourová, concluded the joint review meetings of the EU-US Privacy Shield, with a phone call with US Secretary of Commerce Wilbur Ross.

The aim of the two-day exercise in the US was to investigate how the US commitments are being met through exchanges on the underlying US legal framework in place and on the functioning of the oversight mechanisms. Both sides agreed that the Privacy Shield is key for the data exchanges in transatlantic relations and expressed mutual commitment to making the Privacy Shield a success. Commissioner Jourová said: “The discussions over the past days were fruitful. I appreciate
the commitment the US administration has showed to Transatlantic data transfers and to our concerns. The Privacy Shield can be a win-win for the EU and the US, if implemented correctly." The discussions with the US administration together with feedback from businesses, NGOs and other stakeholders will feed into the Commission's annual review report which will be published in the second half of October. A joint press statement by Commissioner Jourová and US Secretary of Commerce Ross is available online.

Since the program's inception, over 2,400 organizations have joined the Privacy Shield. US and EU officials welcomed the information shared by Privacy Shield participants on Framework compliance, and by civil society and independent recourse mechanism providers. Officials noted that this input greatly informed the review process and will lead to continued improvements to the functioning of the program.

The review examined all aspects of the administration and enforcement of the Privacy Shield, including commercial and national-security related matters, as well as broader U.S. legal developments. Participants also discussed their respective work to implement the Privacy Shield program during its inaugural year, recognizing the value of regular communication between U.S. and EU authorities.

Read more:

Joint Press Statement from US Secretary of Commerce Ross and Commissioner Jourová on the EU-US Privacy Shield Review

European Court of Human Rights reverses ruling on sacking over private messages

On 5 September, the European Court of Human Rights restricted employers’ power to monitor the private messages of their employees.

The Grand Chamber of the European Court of Human Rights held, by eleven votes to six, that there had been a violation of Article 8 (the right to the respect for private and family life, the home and correspondence) of the European Convention on Human Rights. The Court further held that the national authorities had not adequately protected Mr Barbulescu’s right to respect for his private life and correspondence. As a result, they failed to strike a fair balance between the interests at stake.

The ruling overturns a lower court’s decision to back an organisation that sacked an employee for using an instant messaging app for personal reasons

Read more:
Russia threatens to shut down Facebook for non-compliance with local data storage laws

Bloomberg reports that Facebook Inc. will by shut down in Russia next year if it fails to comply with requirements to store user data locally. Roskomnadzor will be forcing foreign internet companies to comply or shut down in the country.

President Vladimir Putin signed a law in 2014 that requires global internet firms to store personal data of Russian clients on local servers. Companies ranging from Alphabet Inc.’s Google to Alibaba Group Holding Ltd complied, while others like Twitter Inc. demanded extra time to evaluate the economic feasibility of doing so.

In November, Roskomnadzor ordered Russian carriers to block access to LinkedIn Corp., citing non-compliance with the law on personal data storage.

Read more:

Bloomberg - Russia Threatens to Shut Facebook Over Local Data Storage Laws

US asks China not to enforce cyber security law

According to Reuters, the United States has asked China not to implement its new cyber security law over concerns it could damage global trade in services.

China ushered in a tough new cyber security law in June, following years of fierce debate around the move that many foreign business groups fear will hit their ability to operate in the country. The law requires local and overseas firms to submit to security checks and store user data within the country.

The United States, in a document submitted for debate at the WTO Services Council, said if China’s new rules enter into full force in their current form, as expected by the end of 2018, they could impact cross-border services supplied through a commercial presence abroad.

“China’s measures would disrupt, deter, and in many cases, prohibit cross-border transfers of information that are routine in the ordinary course of business,” it said.

Read more:

Reuters - US asks China not to enforce cyber security law
Rethinking security when everyone's Social Security number is public

After Equifax disclosed a devastating data breach, much of the attention focused on whether the company did everything it could in response. But the scary truth may be that this is the sort of incident that goes beyond a single company's ability to fix.

Whatever the long-term effects will be, one thing is immediately clear: Social Security numbers are no longer as valuable as they used to be in evaluating consumer identity and creditworthiness.

"[Know Your Customer] requirements were written for a world that expects some privacy of Social Security numbers," said Zach Perret, co-founder and CEO of the fintech company Plaid, at SourceMedia's PayThink event, which took place last week in Phoenix.

Read more:

[Read here](https://www.payingnews.com/2017/09/rethinking-security-when-everyones-social-security-number-is-public) - Rethinking security when everyone's Social Security number is public

Mattel's new gadget for babies sparks privacy concerns

Toymaker Mattel Inc. has announced plans to sell a nursery gadget that will listen to infants and watch over them, record their sleep patterns, and even play a lullaby should they awaken.

Skeptics are asking if the device, similar to Amazon.com's Echo with its Alexa voice assistant, will violate children's privacy and deepen a trend of surrendering intimate human connections to technology that talks and listens.

"The kid tech industry sees kids' bedroom as an economic bonanza," said Jeff Chester, executive director of the Center for Digital Democracy, a Washington-based policy group that advocates for privacy protections. "They can get all kinds of profile information -- the kid likes to eat this kind of food, the kid likes to listen to this kind of music, and we'll have this kind of information that we can share with partners and advertisers."

Read more:

[Read here](https://www.bloomberg.com/news/articles/2017-09-18/mattel-gadget-listens-to-babies-setting-off-privacy-alarms) - Mattel Gadget Listens to Babies, Setting Off Privacy Alarms

Apple revamps "Privacy" site to promote benefits of privacy technologies

Apple has updated its [Privacy mini-site](https://www.apple.com/privacy/) to promote its efforts in safeguarding personal data on its platforms. The
site calls privacy a "fundamental human right" and explains the policies relating to passcodes, Touch ID, Apple Pay, and app permissions. One section addresses "differential privacy," a technology Apple has adopted for mass data collection. Recently, a research paper criticized Apple's differential privacy protections, claiming that they allow too much specific data to pass through, which Apple denies. In addition, according to media reports, Apple has received an inquiry from the U.S. Senate about its new facial recognition technology called Face ID.

On another note, it appears that Apple has received more than four times as many national-security related requests from the U.S. government in the first half of this year versus a year ago. According to CDR Info, which bases itself on Apple's company report, Apple had received between 13,250 and 13,499 national security requests affecting between 9,000 and 9,249 users. That compares with a range of 2,750 and 2,999 requests affecting between 2,000 and 2,249 users in the first half of 2016.

Read more:

Apple - Privacy site

Wired - How one of Apple's key privacy safeguards falls short

CDR Info - Apple Sees Increase in U.S. National Security Requests

Fox News - Apple receives Senate inquiry on Face ID privacy concerns

NotPetya ransomware cost FedEx $300 million

According to Infosecurity Magazine, FedEx has joined the long list of big-name brands that have lost hundreds of millions of dollars after their systems were infected with NotPetya ransomware back in June.

The shipping giant claimed in an earnings call that it would be down approximately $300m following the outbreak, which began in Ukraine and is thought to have spread quickly globally via multi-national companies' VPNs. Subsidiary TNT bore the brunt of the attack, with IT operations still not fully restored.

An earnings statement had the following: "The worldwide operations of TNT Express were significantly affected during the first quarter by the June 27 NotPetya cyberattack. Most TNT Express services resumed during the quarter and substantially all TNT Express critical operational systems have been restored. However, TNT Express volume, revenue and profit still remain below previous levels."

Read more:
Other privacy-related news this month

Infosecurity Magazine - FedEx: NotPetya Cost Us $300 Million

The Guardian - I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets

Chicago Tribune - SEC under fire for being hacked despite warnings on security

Fortune - Sonic’s Stock Plunges After Credit Card Hack That Could Affect Millions

Gizmodo - What Whole Foods Hasn’t Said About Its Payment Card Data Breach

Fortune - After Equifax’s Data Breach, Its CEO Gave a Speech Saying a Hack Was His ‘No. 1 Worry’

BBC News - Deloitte hit by data breach

Future events

What You Need to Know: Threats Your Technology Poses to Confidentiality and Attorney-Client Privilege

Format: Webinar  
Date: October 11, 2017  
Time: 1:00 PM - 2:30 PM ET  
Credits: 1.50 Ethics/Professionalism CLE Credit Hours  
Panelist(s): Aviva Meridian Kaiser, Daniel A Cotter, Jane Whalley Muir  
Moderator: David W Tollen

Technology poses an ever-increasing threat to the attorney-client privilege as well as confidentiality. Emails and social media profiles are usually the culprits when clients or attorneys waive their privilege and inadvertently disclose sensitive information. Additionally, utilizing an employer's technology to communicate can serve as a breach for documents and communication.

The ABA's Model Rules of Professional Conduct should be referenced by attorneys who need guidance on protecting the privilege. This webinar will highlight the pitfalls that should be taken into consideration when using mobile devices, emails, social media, and cloud storage.

Join the panel as they discuss:
- Protecting information while using mobile devices and cloud storage
- Violations to consider when using an employer's
technology for communication
- Educating your client and avoiding inadvertent disclosure

Read more [here](#).

**IP West 2017**

A new forum providing insightful updates on the most current IP Law.

Earn CLE credit while you learn the latest developments in intellectual property law and network with colleagues from the US and around the world.

Leading practitioners will discuss a wide range of IP topics, covering an extensive list of subject areas, including technology, entertainment, life sciences, corporate issues and more.

Highlights include:

- Recent Supreme Court Decisions
- IP Protection in China
- Open Source Software
- Trade Secrets
- Ethics
- Data Privacy
- Trade Dress

Highlights include 3 plenary sessions:
- A judges' panel discussing current bench and bar issues
- A panel with the USPTO and IP practitioners discussing the latest in IP issues
- A corporate issues panel including speakers from Airbnb, Juno Therapeutics, Microsoft, and Nest Labs

Read more [here](#).