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, Nathan M. Barotz and Tamara Lev

---

**European Union: First joint review of Privacy Shield released**

The Article 29 Working Party (WP29) recently released an opinion from its first joint review of the Privacy Shield. The WP29 focused on "commercial aspects of the Privacy Shield" and "government access to personal data transferred from the EU for the purposes of Law Enforcement and National Security."

The WP29 acknowledges the progress of the Privacy Shield in comparison with the invalidated Safe Harbor Decision. The WP29 also recognizes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield. To complement these efforts, the WP29 will engage in advising the U.S. authorities in drafting new guidance, in particular regarding HR data and onward transfers, in order to develop a common understanding of the Privacy Shield Principles and to address the needs of the business community on both sides of the Atlantic.

However, the WP29 has identified a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities. Therefore the WP29 calls upon the Commission and the U.S. competent authorities to restart discussions. An action plan has to be set up immediately in order to demonstrate that all these concerns will be addressed. In particular the appointment of an independent Ombudsperson should be prioritized and the rules of procedure be further explained including by declassification. PCLOB members as well should be appointed. Those prioritized concerns need to be resolved by 25 May 2018.
Other privacy-related news

The WP29 expects the remaining concerns to be addressed at the latest at the second joint review. In case no remedy is brought to the concerns of the WP29 in the given time frames, the members of WP29 will take appropriate action, including bringing the Privacy Shield Adequacy decision to national courts for them to make a reference to the CJEU for a preliminary ruling.

Read more:

Article 29 Working Party - Privacy Shield report, Plenary Meeting November 2017

European Union - New guidelines regarding the principles of consent and transparency

The Article 29 Data Protection Working Party has released its proposed guidelines on transparency, which are open to public comment until 23rd January 2018. The guidelines provide “practical guidance and interpretive assistance” regarding the principles of consent and transparency under the GDPR and set out “general principles” on the rights of data subjects.

Read more:

Article 29 Working Party - Guidelines on Consent under the GDPR

Article 29 Working Party - Guidelines on Transparency under the GDPR

European Union: WhatsApp ordered to stop sharing user data with Facebook

The French data protection authority (CNIL) has issued a formal notice to the company WhatsApp in relation to the transfer of its users’ data to Facebook.

The CNIL considered that the data transfer from WhatsApp to Facebook for “business intelligence” purposes is not based on the legal basis required by French data protection rules for any processing. In particular, it held that the consent is not validly collected because it is not specific to this purpose (when installing the application, users must accept that their data are processed for the messaging service, but also, in general, by Facebook for accessory purposes such as the improvement of its service and it is not free) and the only way to refuse the data transfer for “business intelligence” purpose is to uninstall the application. In addition, the CNIL held that WhatsApp cannot claim a legitimate interest to transfer data to Facebook insofar as this transfer does not provide adequate guarantees allowing to preserve the interest or the fundamental freedoms of users since there is no mechanism whereby they can refuse it while continuing to use the application. As a
result, the CNIL decided to issue a formal notice to WhatsApp to comply with the French Data Protection Act within one month.

In addition, the German Bundeskartellamt has declared that Facebook's collection and use of data from third-party sources is abusive. The authority has announced that it holds the view that Facebook is abusing this dominant position by making the use of its social network conditional on its being allowed to limitless amass every kind of data generated by using third-party websites and merge it with the user's Facebook account. These third-party sites include firstly services owned by Facebook such as WhatsApp or Instagram, and secondly websites and apps of other operators with embedded Facebook APIs.

Andreas Mundt, President of the Bundeskartellamt: "We are mostly concerned about the collection of data outside Facebook's social network and the merging of this data into a user's Facebook account. Via APIs, data are transmitted to Facebook and are collected and processed by Facebook even when a Facebook user visits other websites. This even happens when, for example, a user does not press a "like button" but has called up a site into which such a button is embedded. Users are unaware of this. And from the current state of affairs we are not convinced that users have given their effective consent to Facebook's data tracking and the merging of data into their Facebook account. The extent and form of data collection violate mandatory European data protection principles."

According to the authority's preliminary assessment, when operating this business model Facebook, as a dominant company, must consider that its users cannot switch to other social networks. Participation in Facebook's network is conditional on registration and unrestricted approval of its terms of service. Users are given the choice of either accepting the "whole package" or doing without the service.

Read more:

CNIL - Data transfer from WhatsApp to Facebook: CNIL publicly serves formal notice for lack of legal basis

Bundeskartellamt - Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive

France: Formal notice issued to a manufacturer of connected toys

The French data protection authority (CNIL) has issued a formal notice to the company Genesis Industries Limited to secure its web-connected toys intended for children: the doll "My Friend Cayla" and the robot "I-QUE".
Both toys answer children’s questions on various subjects such as mathematical calculations or concerning the weather. The toys are equipped with a microphone and speaker and are associated to a mobile application downloadable on smartphones or tablets. The answer is extracted from the internet by the application and given to the child through the toys. According to the CNIL, several breaches of the French Data Protection Act have been observed, in particular a violation of the right to privacy because of a lack of security and a lack of information of toys’ users about the data processing carried out and the transfer of data outside the EU.

As a result, the CNIL decided to issue a formal notice to the manufacturer to comply with the French Data Protection Act within two months.

Read more:

CNIL - Connected toys: CNIL publicly serves formal notice to cease serious breach of privacy because of a lack of security

Canada: Canadians have right to privacy in their text messages

Canada's highest court has ruled that an individual does not give up her right to privacy even after she has sent a text message to a third person.

In Nour Marakah v. Her Majesty the Queen (37118), a criminal case in which the defendant, Nour Marakah, was convicted of two counts of trafficking firearms and other charges, the trial court judge had allowed into evidence incriminating text messages from the telephone of one of the defendant's accomplices even though there was no valid search warrant.

In overturning the conviction, the Court stated that "an individual does not lose control over information for the purposes of s. 8 of the Charter [the right to unreasonable search or seizure] simply because another individual possesses it or can access it... Nor does the risk that a recipient could disclose an electronic conversation negate a reasonable expectation of privacy in an electronic conversation. Therefore, even where an individual does not have exclusive control over his or her personal information, only shared control, he or she may yet reasonably expect that information to remain safe from state scrutiny."

Read more:

Nour Marakah v. Her Majesty the Queen

United States of America: Hacker charged in HBO data theft
In a recently released complaint, the U.S. government has charged an Iranian national with stealing protected data from HBO earlier this year. The Department of Justice alleges that Mr. Behzad Mesri, who had previously performed work for the Iranian military in conducting computer network attacks targeting military systems, nuclear software systems, and Israeli infrastructure, and was a member of the hacking group Turk Black Hat Society, stole “unaired episodes of original HBO television programs, including episodes of 'Ballers,' 'Barry,' 'Room 104,' 'Curb Your Enthusiasm,' and 'The Deuce';’ scripts and plot summaries for unaired programming, including but not limited to episodes of ‘Game of Thrones;' confidential cast and crew contact lists; e-mails belonging to at least one HBO employee; financial documents; and online credentials for HBO social media accounts.”

Mesri demanded a ransom of $6 million dollars in bitcoin or he threatened that he would release the stolen data and destroy additional data on the HBO computer servers. Mr. Mesri is charged with, among other counts, three counts of computer fraud.

Read More:

Press Release - Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO

Scanned indictment U.S. v. Behzad Mesri

**United Kingdom: Vicarious liability for innocent data controllers following employee’s theft of personal data**

A U.K. High Court judge has ruled that the British supermarket chain Morrisons is vicariously liable for an employee’s theft of the payroll data of nearly 100,000 employees which included personal data such as employee names, addresses and bank account details.

In a 59 page decision in *Various Claimants v WM Morrisons Supermarket PLC* (case number HQ15X05099 in the High Court of Justice, Queen's Bench Division), the Honorable Mr. Justice Langstaff set forth the history of the case. In 2014 Mr. Andrew Skelton was a Senior IT Auditor in Morrisons’ employment and had the responsibility to pass the employee data onto KPMG as part of Morrisons annual audit process. Mr. Skelton stole the data and posted it on a file sharing website. In 2015 Mr. Skelton was charged with violations of the Computer Misuse Act of 1990 and Data Protection Act of 1998, convicted of the theft and sentenced to eight years in prison. A class of 5,518 Morrisons’ employees sued Morrisons in 2015 seeking damages for alleged violations of the Data Protection Act, misuse of private information and breach of confidence.
After a lengthy finding of facts, the court held that "the DPA [Data Protection Act of 1998] does not impose primary liability upon Morrisons; that Morrisons have not [sic] been proved to be at fault by breaking any of the data protection principles, save in one respect which was not causative of any loss; and that neither primary liability for misuse of private information nor breach of confidentiality can be established." The court went on to state that "Morrisons did not directly misuse any information personal to the data subjects. Nor did they authorise [sic] its misuse, nor permit it by any carelessness on their part. If Morrisons are [sic] liable it must be vicariously or not at all."

The court applied standards set forth in *Mohamud v William Morrison Supermarkets plc* [2016] UKSC11 to determine if Morrisons was vicariously liable. The court had to determine "whether there was sufficient connection between the position in which he was employed and his wrongful conduct to make it right for the employer to be held liable under the principle of social justice." The court concluded that Mr. Skelton's actions were sufficiently closely connected to the responsibilities assigned to him that Morrisons was vicariously liable for his actions.

Read more:

[Various claimants -v- WM Morrisons Supermarket PLC](#)

**Philippines: Privacy office readying to flex enforcement muscle**

The Philippines privacy office should become fully operational by mid-2018 and will step in to protect the privacy rights of Filipino data subjects wherever in the world violations occur, the country’s privacy chief told Bloomberg BNA in an interview.

Companies doing business in the Philippines, including those that handle customer service and data processing functions for companies outside the country, may face more focused privacy and data security enforcement as a result.

The Philippines sees effective data protection as fundamental to underpin the expansion of its vital business processing operations sector (BPO), which provides call centers, data transcription, and similar services carried out on behalf of foreign corporations, Privacy Commissioner Raymond Liboro said on the sidelines of the 39th International Data Protection and Privacy Commissioners' Conference in Hong Kong.

Read more:

[Bloomberg - Philippines Privacy Office Readying to Flex Enforcement Muscles](#)
South Korea: Biometric information protection guidelines released

The Korea Communications Commission ('KCC') released, on 12 December 2017, biometric information protection guidelines aimed at providing operators of such information with clarity on how to implement measures necessary for the protection of biometric information.

The Guidelines propose six protection principles and technical and administrative measures necessary for the protection of biometric information. In particular, the Guidelines include, among other things, the principle of collection and use of biometric information, to which operators must clearly inform and agree with users the purpose of collecting and using biological information, the period of retention, and that the original information should be destroyed after generating the information. Moreover, the Guidelines include the principle of restricting purpose, to which biometric information agreed to by users for authentication or identification should not be used for other purposes without permission and to use biometric information for other purposes, it is necessary to follow legal procedures such as prior consent. Furthermore, the technical and administrative measures are provided in the Guidelines to assist implementation to prevent leakage, forgery and alteration to biometric information.

Read more:

Korea Communications Commission Press Release (Korean only)

Guidelines (Korean only)

United States of America: Who has standing?

Last month the Ninth Circuit Court of Appeals affirmed the lower court decision in Eichenberg v. ESPN, Inc.. In Eichenberg, the plaintiff brought a claim under the Video Privacy Protection Act alleging that ESPN had violated the act by sharing the serial number of the plaintiff's Roku device with the analytics firm, Adobe. ESPN argued that Eichenberg did not have standing because he did not allege a concrete harm. In affirming the lower court, the appellate court held that the Eichenberg did have standing under the statute and stated that "that every disclosure of an individual's 'personally identifiable information' and video-viewing history offends the interests that the statute protects, and that the plaintiff need not allege any further harm to have standing." The appellate court did, however, affirm the lower court's decision dismissing the claim by holding that the serial number alone did not constitute information that was "capable of identifying an individual."

Also last month and in contrast to Eichenberg, the
Second Circuit Court of Appeals ruled that the plaintiff in Santana et al v. Take-Two Interactive Software, Inc. lacked standing to sue over the collection of biometric data because the plaintiffs had failed to show injuries or at least a real risk of harm. The plaintiffs alleged a violation of the Illinois Biometric Information Privacy Act of 2008. The plaintiffs, who had their faces scanned, alleged that Take-Two had failed to obtain their informed consent and argued that the defendant was storing their facial geometry data. The court examined whether the plaintiffs had either constitutional standing or properly stated a cause of action under the state law. In finding that the plaintiffs did not have constitutional standing, the appellate court focused its inquiry on any presentation of a "material risk of harm to a concrete interest." The decision notes that Take-Two informed game-players that a "face scan" would be required for the personalized virtual basketball player feature and that the game company met standards for informed consent. The appellate court rejected the defendants' arguments that Take-Two did not inform them of the duration that it would hold their biometric data, as the law required, as the court did not see a material risk presented that their data will be misused or disclosed. "Plaintiffs have not alleged that Take-Two has not or will not destroy their biometric data within the period specified by the statute, and accordingly have alleged only a bare procedural violation," states the decision. "Likewise, although Take-Two did not notify the plaintiffs of its 'retention schedule and guidelines for permanently destroying [their] biometric [data],' id., plaintiffs do not allege that Take-Two lacks such protocols, that its policies are inadequate, or that Take-Two is unlikely to abide by its internal procedures." With regards to the Illinois statute, the court recognized that alleged violations of the Illinois law's data security provisions "raise a somewhat thornier issue," pointing to allegations that Take-Two transmitted face scans using less than secure networks. But the court held that the plaintiffs still did had not done enough. "Despite multiple opportunities to amend their pleadings, plaintiffs have failed to allege that Take-Two's alleged violations have raised a material risk that their biometric data will be improperly accessed by third parties. They therefore have failed to show a 'risk of real harm' sufficient to confer an injury-in-fact."

Read more:

Chad Eichenberger v. ESPN Inc.

Santana et al v. Take-Two Interactive Software, Inc.

Other privacy related news

A new global study released by Pegasystems revealed 82 percent of European consumers plan to exercise their new rights to view, limit, or erase the information businesses collect about them. While awareness of GDPR itself is low today, consumers are overwhelmingly...
interested in querying companies that hold their personal information. For example, 90 percent want direct control over how companies use their data, while 89 percent want to see the data companies store on them. Read more: EU Consumers Poised to Take Back Control of Personal Data from Businesses, According to Pega Survey on GDPR

Amazon Echo (also known as “Alexa”) has become quite popular in most homes today. Alexa is always listening, just by saying her name, your wish is her command. She hears, listen and obeys as her owner dictates, which can lead to some nifty privacy issues. As the holidays approach and the gifts come pouring in, here are some tips and tricks to make sure you stay safe and sound from the famous Alexa. Read more: 3 Essential Privacy Settings for Your Amazon Echo

Firefox users last week started noticing that a mysterious extension called “Looking Glass” had been added to their browsers. The extension’s description included the ominous phrase “My Reality is Different Than Yours.” There was some speculation that it was a form of malware, but users quickly identified it as part of a promotion for the USA Network hacker-conspiracy show Mr. Robot. The problem is that the extension, which transformed some text and added game clues to certain websites, was installed without user opt-in, except to a program called Shield Studies that enabled Firefox’s creators to gather data for improving the browser. That permission is reportedly enabled by default for at least some users. Read more: Firefox Users Cry Foul Over ‘Mr. Robot’ Ad Installed As Research Program

4iQ’s (data security company) most recent find, is a 41 gigabyte file that contains 1.4 billion usernames and passwords on the dark net. While everything is alphabetized and organized in clear text, one of the main issues is that the information did not come from one source. The username and passwords have been collected from multiple places which include: Netflix, LinkedIn, MySpace, and more. Even though some of these breaches happened a while ago, this is nonetheless disturbing due to the fact that most people “recycle” or reuse password on a constant basis. Read more: File with 1.4 Billion Hacked and Leaked Passwords Found on the Dark Web.

Email tracking is evolving, so much so that one in every five email a person receives is being tracked. In the body of the email there is a 1x1 pixel image, that is so small an individual cannot see it. Once the recipient opens the email, the tracking client knows on what device the email was opened, the IP address, and location of the device. As the article points out: “All of this means that billions of emails are sent every day to millions of people who have never consented in any way to be tracked, but are being tracked nonetheless”. Read more: How Email Open Tracking Quietly Took Over the Web
Apparently Netflix knows what you're up to this holiday. Netflix went on a rant on Twitter regarding their film for the holidays, asking why 53 people watched the same exact movie for 18 days straight. Read more: Netflix Just Roasted 53 Fans of A Christmas Prince

One of this year's hottest holiday gifts has privacy advocates worried. In Tucson and elsewhere, sales of home DNA testing kits are soaring, spurred by discount pricing and ubiquitous TV ads that promise users insights into their family heritage. But the saliva tests can also reveal propensities for diseases, and critics fear users may be putting their medical privacy at risk by providing genetic information to companies that can't guarantee it will remain anonymous. Read more: DNA tests a hot holiday item despite privacy concerns

### Future events

**Preparation is the Key: Digital Media Forensics 101**

**Format:** Webinar  
**Date:** January 9, 2018  
**Time:** 1:00 PM - 2:30 PM ET  
**Credits:** 1.50 General CLE Credit Hours  
**Panelists:** Craig Ball, G Hunter Jones, Jiyun Cameron Lee, Kimberly Metzger

Computer files and other Electronically Stored Information (ESI) are now an important element in virtually every civil proceeding and a great many criminal cases as well. Obtaining, searching, understanding, and explaining the fruits of production require increasing amounts of highly specialized knowledge.

Few practicing attorneys have the opportunity (or the time) to keep up in these evolving fields. Computer Forensics is necessarily a joint responsibility between counsel and the analyst.

The attorney doesn't need full training in Computer Science, but will need to know enough about the place of Computer Forensics in the type of cases he or she handles, in order to recognize the capabilities of such analysis and how to find and work with qualified experts.

Forensic methods routinely expose materials that are not evident through simple examination:

- Valuable hidden information (metadata) within documents;  
- Extensive record of user activity captured in computers, tablets and phones;  
- Full or partial content of "deleted" documents, Emails, and texts.

In addition to finding information for your own case, you will often need to have an expert to review the findings.
presented by experts for prosecutors or opposing counsel. Even when the viewable evidence is the same, different reviewers will have different conclusions, as the technical details are so complex that many misinterpretations are properly overturned by rebuttal witnesses.

Read more here.

Editors

**Paul Lanois** - Mr Lanois is a global privacy, data protection and information security professional and is an attorney admitted to the Bars of the District of Columbia (DC-USA), New York (NY-USA) and the Supreme Court of the United States (SCOTUS). He regularly publishes articles on technology law and is frequently invited to speak on such topics. He has spoken at conferences across Europe, Asia and the United States. He was named a "Cybersecurity & Data Privacy Trailblazer" by the National Law Journal and an "Innovative Corporate Counsel" by Law 360. He was also recognized as a leading lawyer in The Legal 500’s GC Powerlist. He has been recognized as a Fellow of Information Privacy (FIP) by the International Association of Privacy Professionals (IAPP) and is a Certified Information Privacy Professional, with concentrations in Asian law (CIPP/A), US law (CIPP/US), European law (CIPP/E) and Canadian law (CIPP/C). He is also a Certified Information Privacy Manager (CIPM) and a Certified Information Privacy Technologist (CIPT). 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 and Linklaters). 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 a Certificate in Business and Public Policy from the Wharton School at the University of Pennsylvania.

**Nathan M. Barotz** - Mr. Barotz has been in the private practice of law for over 25 years. A graduate of Duke University (cum laude) and the George Washington University Law School, Mr. Barotz originally developed a focus on health care law which in the last ten years has led to his strong interest the rapidly developing body of law governing IoT, cybersecurity and privacy. For the last five years, Mr. Barotz has served in the role of general counsel and compliance and privacy officer for companies utilizing telemedicine technology in post-acute patient treatment and currently serves in that role for HomeSleep, LLC, a company which specializes in diagnostic testing for sleep apnea. Mr. Barotz is a member of the New York State and Connecticut State Bars, the United States District Court Bars, Southern District and Eastern District of New York and has received his CIPP/US certification.
from the International Association of Privacy Professionals.

**Tamara Lev** - Ms. Lev is a consultant specializing in data privacy, information security, and regulatory compliance. She assists her clients with diligence and care, while identifying potential privacy vulnerabilities and conducting information security risk assessments. Tamara is a law graduate from Ono Academic College with a LLB in Law. She is a Fordham Law School graduate with a LLM in Intellectual Property and Information Technology. Tamara is a member of the State Bar of New York.