Foreword

The hot topic this month in the area of privacy is undoubtedly the announcement of the new "EU-US Privacy Shield", which would replace the 15-year old "Safe Harbor" pact (see below for more details on the Privacy Shield). According to the Safe Harbor website, over 4,000 companies are registered under the program. What should we expect for the Privacy Shield? Should it be seen as nothing more than a "Safe Harbor 2.0"? Assuming that the EU Commission approves the Privacy Shield, is it the end of the story, or has the story only just begun?

As surprising as it may seem, one of the key findings of the Court of Justice of the European Union (CJEU) in the Maximillian Schrems v Data Protection Commissioner is not that the EU-US Safe Harbor was found to be invalid under EU data protection rules. Rather, a key finding was that the Data Protection Authority (DPA) of a EU member state should examine whether any transfer of personal data to a territory outside the European Economic Area (EEA) provides an "adequate" level of protection, without any limitation.

The CJEU clearly states, on line 66, that a decision "by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection" (bold added for emphasis).

In other words, the CJEU's holding is that any international pact or agreement or even a decision from the EU Commission would not prevent a DPA from assessing whether an adequate level of protection really exists in relation to a transfer of personal data to any country or territory outside the EEA. Thus, the transfer of information to a country or territory outside the EEA other than the US could potentially be invalidated, even if the EU Commission has previously issued an adequacy decision. Likewise, any framework for the transfer of personal data outside the EEA could potentially be invalidated.

This is probably the reason why the WP29, which is an advisory group composed of representatives from the DPAs of each EU member state, has stated in February 2016 that the essential guarantees "should be respected whenever personal data are transferred from the EU to the United States and to other third countries, as well as by EU Member States" (bold added for emphasis).

The WP29 further added that it "will consider whether transfer mechanisms, such as Standard Contractual Clauses and Binding Corporate Rules, can still be used for personal data transfers to the US" (bold added for emphasis).

In other words, even Standard Contractual Clauses and Binding Corporate Rules could potentially be held as being invalid under EU data protection rules, if it is determined that an adequate level of protection is not ensured.

Of course, there is no indication at this stage that these mechanisms do not offer an adequate level of protection under EU data protection rules, nor is there any reason to believe that a DPA would make such a finding - in fact, the WP29 has indicated in the
same February statement that those transfer mechanisms are still deemed to be acceptable. The fact that President Obama has just signed the Judicial Redress Act into law is certainly a step in the right direction, but as stated in the Schrems decision, that would probably not prevent a supervisory authority of an EU Member State from making its own assessment on whether or not an adequate level of protection is provided. It appears that nothing should be taken for granted and everything is subject to change. Adopting any transfer mechanism should therefore be carefully considered and assessed.

We hope that you enjoy reading this newsletter as much as we enjoyed preparing it. Please do not hesitate to contact us about any ideas you may have for this newsletter.

Paul Lanois

**VTech data breach fallout**

Following the security breach at electronic toy maker VTech (reported in our previous newsletter), the company has recently updated its Terms of Service.

In particular, new clauses have been added, such as "You acknowledge and agree that any information you send or receive during your use of the site may not be secure and may be intercepted or later acquired by unauthorized parties. You acknowledge and agree that your use of the site and any software or firmware downloaded therefrom is at your own risk. Recognizing such, you understand and agree that, to the fullest extent permitted by applicable law, neither VTech nor its suppliers, ..., other partners or employees will be liable to you for any direct, indirect, incidental, special, consequential, punitive, exemplary or other damages of any kind..."

Despite widespread criticism and calls for a boycott of the products, the company has refused to back down from these changes. What weight should be granted to such limitations of liability? Can contractual clauses really be used to absolve security responsibility?

The terms do include the caveat that the company may only be held liable to the "extent permitted by applicable law". However, any entity that collects, stores or processes personal data has a legal obligation to ensure the protection of such data against accidental or unlawful destruction, loss, alteration or disclosure.

The UK’s DPA (the Information Commissioner’s Office) has already weighed in on the issue, confirming that organisations handling personal data are of course responsible for keeping the data secure. Going forward, the EU General Data Protection Regulation will continue imposing responsibility on organizations handling personal data, since it will impose fines of up to 4% of the company’s gross revenue to be paid in the event of a data breach, regardless of the content of the terms of service.

**The Privacy Shield: "Safe Harbor 2.0"?**

On February 2, 2016, the EU and US authorities announced that they reached an agreement on a new transatlantic data transfer framework, referred to as the "Privacy Shield". Representatives from both the EU and the US have been negotiating the terms of the agreement since October 2015, when the CJEU invalidated the Safe Harbor Framework in the case of Maximillian Schrems v Data Protection Commissioner. The Privacy Shield seeks to bring over 4,000 companies into compliance with EU privacy laws by placing stronger obligations on companies handling EU citizens data, making government data access more transparent, and permitting EU citizens to seek redress of violations of their privacy rights.

Now that the agreement has been reached, it must be submitted to the EU Commission for approval. In doing so, the EU Commission must consider, among others, the opinion of the Article 29 Working Party (WP29). While the opinions of the WP29 are not binding, they are persuasive. In a statement issued on February 3, 2016, the WP29
requested the opportunity to review documents pertaining to the Privacy Shield and issued four essential guarantees that should be preserved under any framework. If the WP29 and the DPAs reject the Privacy Shield, it is extremely likely that the CJEU would adopt a similar view. Until the Privacy Shield is fully adopted, companies have been encouraged to continue using EU-approved model contract clauses and Binding Corporate Rules (more info regarding alternative contracts).

Privacy advocates in the EU and the US have overwhelmingly reacted negatively to the announcement of the Privacy Shield. Since the actual text or details of the agreement have not yet been released, some have questioned whether the agreement is no more than a “Safe Harbor 2.0”. Max Schrems, who brought the case originally, has stated that a couple of letters by the outgoing Obama administration is by no means a legal basis to guarantee the fundamental right of 500 million European user in the long run.

The Electronic Privacy Information Center (epic.org) attempted to gain access to a copy of the Privacy Shield through the Freedom of Information Act (FOIA), however the US Department of Commerce has responded that the record does not yet exist. Others believe that agreement will inevitably end up before the CJEU, just like its predecessor.

Currently, the Privacy Shield is being reviewed by WP29 and the DPAs of each EU nation. In the US, Congress has passed the Judicial Redress Act, which has been sent to the White House. A portion of this bill allows EU citizens the right to challenge the misuse of their data in American courts. President Obama has signed the Judicial Redress Act into law. While the passing of this bill is a step in the right direction, it is certainly not a final solution for securing the validity of transatlantic data transfers.

A final decision on the Privacy Shield is expected from the European Commission and the EU DPAs in late May or early April.

See also: WCL IP Brief.

**Encryption out of reach for law enforcement?**

Since the Snowden revelations in 2013, U.S. law enforcement has been fighting the Silicon Valley and privacy groups about encryption technology. Law enforcement argues that encryption hinders their ability to quickly move on targets and that government should be able to get to decrypted information. In response, tech companies and privacy advocates have argued that encryption provides greater security for users and the creation of “backdoors” into encryption systems would undermine trust and make systems vulnerable to new attack vectors.

However, the assumption appears to be that criminals and terrorist using encryption to secure their own communications would be using encryption systems created by US companies. While this is possible, this may not necessarily be the case in every instance since it appears that roughly two-thirds of encryption services are created outside the US, making most of the world’s encryption out of reach for US law enforcement. Therefore, if US companies were forced to implement backdoors, it is likely that criminals and terrorist alike would move off of American systems and use encryption outside the US. Thus, any changes to U.S. regulations creating back doors would likely not solve the issue. Instead, these holes in the system would solely leave networks with additional vulnerabilities.

The encryption debate took another turn when four bipartisan members of the U.S. House of Representatives introduced in February a bill prohibiting states from creating law requiring companies to build encryption weakness into the system. The Ensuring National Constitutional Rights for Your Private Telecommunication Act, or the ENCRYPT Act, seeks to prevent any state or locality from forcing any manufacturer, developer, seller, or provider to design or alter a security products such that it could be decrypted or monitored by authorities. The legislation came in direct response to
individual states taking actions to regulate encryption technology.

Even more recently, a federal judge in California ordered Apple on 16 February 2016 to help the government unlock and decrypt the iPhone 5C used by Syed Rizwan Farook, one of the terrorists involved in an attack in San Bernardino, California, on December 2, 2015. This court order has sparked a number of comments, including from Congressman Ted Lieu, the EFF or the New York Times. Apple has already issue a statement. A number of tech leaders have weighed in on the issue. Cyber-security pioneer John McAfee has even personally offered to crack the iPhone for free so that Apple does not need to create a back door on its products.

Interestingly, Apple has already separately requested a federal court in New York to rule on whether it can be compelled to unlock the iPhone 5S of an alleged methamphetamine dealer.

**Hackers leak private files of police union**

Private files belonging to the Fraternal Order of Police ("FOP"), including the names and address of officers, forum posts and controversial contacts with city authorities were posted on January 28 after a hacker breached its website. The police union says the FBI is investigating after 2.5GB of data were taken from its servers, placed online and quickly shared through social media.

Chuck Canterbury, national president of the FOP stated that he's confident no sensitive personal information or financial details of the members had been obtained. The FBI declined to comment on its ongoing investigation, but the FOP had called in security contractors to investigate the hack who traced it to an IP address in the UK.

Canterbury stated that the hackers were able to feed their system a "pseudo-encryption key" that the system should not have accepted but did because of software errors.

Source: The Guardian

**Security news updates**

**California data breach report issued**


The report found that between 2012 and 2015, there were 657 data breaches, which compromised over 49 million records of Californians’ personal information. The report is accompanied by recommendations for organizations, businesses and lawmakers on how to protect against data breaches, and points to a specific set of actions that companies and organizations should start with to meet the state and federal mandates of reasonable security.

Although the report only relates to California, it is likely that, given the size of the state of California, the document would have an impact on large companies doing business in the U.S. In particular, the report states that “the 20 controls in the Center for Internet Security’s Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.”

Source: California data breach report

**Ukrainian hacker linked to U.S. cyber-security expert pleads guilty**
A Ukrainian computer hacker named Sergey Vovnenko, also known as "Flycracker" and "Centurion", pleaded guilty to charges of aggravated identity theft and conspiracy to commit wire fraud.

Vovnenko faces a mandatory minimum two-year prison term and may face additional time plus a fine at his sentencing on May 2. Prosecutors said that between September 2010 and August 2012, Vovnenko was part of an international conspiracy intending to hack computers belonging to individuals and companies in order to steal debit and credit card numbers. Vovnenko admitted operating a "botnet" that infected more than 13,000 computers with malware, giving him unauthorized access to steal banking information and record keystrokes.

Vovnenko is linked to Brian Krebs, a well-known journalist and cyber-security expert. In 2013, Krebs foiled a plot by Vovnenko to have heroin sent to Krebs' home and notify the police once it arrived. Krebs tracked Vovnenko's online activities and alerted the police.

Source: Reuters

US to rework arms control rule on exporting hacker tools

The Department of Commerce, Bureau of Industry and Security is re-writing a proposal under the arms control rules to make it easier to export tools related to hacking and surveillance software, since these tools are also used to secure computer networks. The White House supports making cyber intrusion tools available overseas for legitimate uses. Industry groups and legislators have raised concerns that limiting the spread of such tools may have unintended negative consequences for national cyber-security and research.

Caroline Tess, National Security Council Senior Director for Legislative Affairs said that the White House has intensified its discussion with U.S. officials and industry and that the Department of Commerce will await an additional round of public comment on the revised draft before issuing a final rule. In May, the Department of Commerce proposed denying the transfer of offensive tools - defined as software that uses "zero-day" exploits or unpatched new vulnerabilities and "rootkit" abilities that provide administrator-level access to a system.

The draft rule provoked nearly 300 comments from cyber-security professionals, activists and lawmakers who said it would weaken cybersecurity. The Bureau of Industry and Security is working on new language and it is expected sometime in the first half of the new year.

Source: USNews

New US Cyber-security National Action Plan

On February 9, 2016, the Obama Administration released a Cybersecurity National Action Plan. The plan directs the Federal Government to take active steps to increase cyber-security across the federal government by modernizing Government IT systems, establishing a Federal Chief Information Security Officer, and increasing collaboration with the private sector. CNAP includes a FY2017 budget increase of $19 billion, with $3.1 billion for an Information Technology Modernization Fund. While the Plan proposes increased private sector collaboration, it does not mandate any actions by the private sector. Overall, the plan seeks to improve incident response, secure technology, and enhance critical infrastructure while simultaneously ensuring privacy and transparency.

Sources:
White House Press Release
National Law Review
Upcoming events

**National Institute on the Internet of Things**

With an estimated 75 billion connected (aka “smart”) devices to be in place by 2020, the Internet of Things (“IoT”) is potentially one of the fastest emerging, transformative, and disruptive set of technologies introduced in recent years. IoT devices are already having significant technical, social and economic impact on our connected lives. Defined with deceptive simplicity, the IoT is the interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data. These devices and sensors, which include wearables, ingestibles, systems inside moving vehicles, smart cities, home controllers and security systems, energy management, standardized and customized production environments, and mass transportation infrastructure, also bring into focus new lifespan and upgradeability issues, including security, authentication, privacy, data ownership and potential product liability on a massive scale. The disruptive growth of the IoT will require the participation of all nonconsumer stakeholders (manufacturers, vendors, regulators and legislators) to address potential risks and liability. This ground breaking conference will offer attendees an IoT deep dive, providing incisive and cutting edge insight from legal and technology experts in the field.

**Format**: In-Person  
**Location**: Jones Day, 51 Louisiana Ave NW Washington, DC 20001-2113  
**Date**: March 30-31, 2016  
**Credits**: 12.50 General CLE Credit Hours, 1.00 Ethics / Professionalism CLE Credit Hours

Register here for the National Institute on the IoT.

**Cloud Computing 201: Key Issues and Practical Guidance for Negotiating Cloud Contracting in 2016**

ABA Value Pass 1.00 CLE Format: Webinar  
**Time**: 1:00 PM - 2:00 PM ET  
**Add to Calendar**  
**Panelist(s)**: Edward Paddock III, Janet Stiven, Mark Wesley Irving  
**Moderator(s)**: Joseph M Pennell

Organizations are increasingly viewing the cloud as their first choice when contracting for IT and technology services. This program will help practitioners understand how the cloud is impacting “standard” contract terms (such as limitations of liability), rights upon termination, security obligations, data location (especially in light of the “Safe Harbor” ruling in Europe), and what to expect in real-world negotiations with cloud service providers.

**Format**: Webinar  
**Panelists**: Edward Paddock III, Janet Stiven, Mark Wesley Irving, Joseph M Pennell  
**Date**: March 9, 2016  
**Time**: 1:00 PM - 2:00 PM ET  
**Credits**: 1.00 General CLE Credit  
**List Price**: $195.00  
**ABA Member Price**: $150.00  
**Sponsor Member Price**: $95.00

Click here to register for Cloud Computing 201.

**IAPP Global Privacy Summit 2016**

In the privacy sphere, amidst increasing risk, evolving regulatory requirements and
rising customer expectations, there’s strength in numbers.

Enter the Global Privacy Summit, drawing us in, taking a spotlight to the challenges of our time. Here, we grow our knowledge, make surprising, valuable connections and, most importantly, advance the privacy conversation together.

The Summit remains the largest and most-anticipated privacy event in the world, and the 2016 program will not disappoint. The stage is set: Don’t miss the show.

**Format:** In-Person  
**Location:** Washington DC  
**Date:** April 3-6

Click here for more information on the [IAPP Global Privacy Summit 2016](#).

### Publication feature


With the understanding that the law and the technology it regulates form a complex and intertwined bond, this book covers both the laws of unmanned aircraft and the respective technological foundations required to understand and work with the law in an informed manner.

Unmanned aircraft law is a subset of aviation law, with its own unique perspective. As such, aviation law foundations are critical to the unmanned aviation legal scholar/practitioner and are covered appropriately throughout the book.

Also covered are the legal foundations of insurance and risk, product liability, system security, information assurance, and safety. Additionally, this book has a section on Constitutional law, covering emerging areas that may impact civil rights and civil liberties, as well as issues concerning the media, such as freedom of the press and freedom to cover stories involving collaboration with law enforcement.

In essence, this book brings together the legal, technological, and operational perspectives of drone and unmanned aircraft law into one comprehensive resource.