Foreword

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

Appeals Court Upholds ESPN Win in Video Privacy Suit

A federal appeals court has upheld a win for ESPN Inc. in a lawsuit that accused the company of sharing the personal identities of customers who used the sports network’s Roku streaming application with data analytics companies.

The plaintiff, Chad Eichenberger, attempted to bring a claim under the Video Privacy Protection Act, alleging that ESPN had disclosed the videos he was watching by sharing the serial number of his Roku device with the analytics firm, Adobe.

Read more:
Hollywood Reporter - Appeals Court Gives ESPN a Win Despite Opening Door to More Privacy Lawsuits

Canadian federal court denies request from Canadian Security Intelligence Service for telecom subscriber info

A federal judge in Canada has rejected the request from the Canadian Security Intelligence Service (CSIS) to obtain basic information about unknown phone and internet subscribers who may come to the intelligence agency's attention in the future.

Canadian federal court Chief Justice Paul Crampton said
the CSIS failed to show a sufficient connection between its investigation and the people whose privacy rights would be compromised. As part of a terrorism investigation, CSIS was seeking judicial warrants for the names and street addresses of telecom subscribers and, in some cases, information relating to IP addresses. The subscriber information related to telephone numbers or electronic identifiers that might one day come to the agency’s attention in the course of its probe.

Read more:

CBC News - CSIS’s ask for telecom subscriber info of possible future targets denied

Top EU privacy watchdog wants centralised privacy regulator to investigate and sanction companies

EU lawmakers should create a new, centralised data protection authority to oversee investigations of privacy breaches that affect more than one member state in the bloc, Giovanni Buttarelli, the European Data Protection Supervisor, said in an interview.

National watchdogs policing data protection, consumer rules and competition often confront companies with similar complaints, and a central authority should do away with that fragmentation, Buttarelli said. The change could be a long-term move that would require new EU privacy legislation and more power for a single regulator to investigate and sanction companies.

Read more:

Euractiv - Top EU privacy watchdog wants centralised regulator with muscle to police firms

European Court of Human Rights holds that camera surveillance of university lecture halls violates privacy

In the case of Antović and Mirković v. Montenegro (28 November 2017), the European Court of Human Rights held that camera surveillance in lecture halls at the University of Montenegro’s School of Mathematics violated Article 8 of the European Convention on Human Rights (the right to respect one’s "private and family life").

The case concerned an invasion of privacy complaint by two professors at the University of Montenegro’s School of Mathematics, Nevenka Antović and Jovan Mirković, after video surveillance had been installed in areas where they taught. They stated that they had had no effective control over the information collected and that the surveillance had been unlawful. The local courts rejected a compensation claim, since the auditoriums where Antović
and Mirković taught were public areas.

The Court stated that it had previously found that “private life” might include professional activities and considered that was also the case with Antović and Mirković. Article 8 was therefore applicable. On the merits of the case, it found that the camera surveillance had amounted to an interference with their right to privacy.

Read more:

European Court of Human Rights - Case of Antović and Mirković v. Montenegro

European Court of Human Rights Press Release

Human Rights Europe - Court: Camera surveillance of Montenegro lecture halls violated professors' privacy

Dutch DPA: unlimited publication of WHOIS-data violates privacy law

The Dutch Data Protection Authority, Autoriteit Persoonsgegevens, has stated that the unlimited publishing of data belonging to individuals who have registered domain names is a violation of Dutch and European privacy law.

Based on the rules issued by ICANN, the worldwide domain name administrator, the Dutch registry is required to publish WHOIS-data on the internet with unlimited access, including the name, address, email address and telephone number of the person who has registered a domain name. However, according to the Dutch authorities, the unlimited publication of personal data of domain name registrants is a violation of Dutch and European privacy rules since the unlimited publication of these personal information on the internet is not necessary and access should be restricted to when it is strictly necessary for technical reasons, or for law enforcement when it is legally entitled to such access.

The Dutch authorities further reminded that the other European data protection authorities, assembled in the Article 29 Working Party (WP29), have already expressed their concerns about the unlimited publication of personal data of domain name registrants.

Read more:

Autoriteit Persoonsgegevens Press Release - Dutch DPA: unlimited publication of WHOIS-data violates privacy law

Australia announces participation in APEC CBPR

Australia has announced that it will participate in the APEC Cross Border Privacy Rules (CBPR) system. The
CBPR System was developed by participating APEC economies with the aim of building consumer, business and regulator trust in cross border flows of personal information.

It requires participating businesses to develop and implement data privacy policies consistent with the APEC Privacy Framework. These policies and practices are assessed against the minimum program requirements of the APEC CBPR system by an Accountability Agent (which is an independent APEC recognised private sector entity). By applying a commonly agreed upon baseline set of rules, the CBPR system bridges differences that may exist between different domestic privacy approaches.

In July 2017, the Australian Government invited businesses and other interested stakeholders to comment on a discussion paper about the implications of Australia’s possible participation in the CBPR system.

Read more:

Australian Government Attorney General's Department - APEC Cross Border Privacy Rules public consultation – Australia’s participation

India releases white paper on proposed data protection framework

Following the landmark judgement of the Supreme Court in Puttaswamy (August 2017), which recognized the right to privacy as a fundamental right and required the establishment of a data protection regime to protect the privacy of the individual, the government of India has formed a committee of experts under the Chairmanship of former Supreme Court Justice Shri B N Srikrishna to study various issues relating to data protection in India and make specific suggestions on principles to be considered for data protection in India and suggest a draft Data Protection Bill. The objective is to “ensure growth of the digital economy while keeping personal data of citizens secure and protected.”

A white paper has been drafted to solicit public comments on what shape a data protection law in India must take. The white paper outlines the issues that a majority of the members of the Committee feel require incorporation in a law, relevant experiences from other countries and concerns regarding their incorporation, certain provisional views based on an evaluation of the issues vis-à-vis the objectives of the exercise, and specific questions for the public.

Proposals put forward by the white paper include covering cases where processing partly takes part in India even if the processing is carried out by non-Indian entities that do not have a presence in India, and regulating entities which offer goods or services in India even if they do not have a presence in India (modelled
on the EU GDPR).

Read more:

White Paper of the Committee of Experts on a Data Protection Framework for India

**UK supermarket liable for data breach by disgruntled staff member**

UK supermarket Morrisons has been found liable for a former employee leaking personal information about nearly 100,000 members of staff, despite the court finding that Morrisons had provided “adequate and appropriate controls” and did not know or ought to have known that Skelton bore a grudge against the company and posed a threat. This landmark case could therefore prompt companies to further limit workers’ access to data.

In the UK’s first data protection class action, thousands of staff sued Morrisons after their personal details were leaked online by a senior IT employee, Andrew Skelton, in 2014. Information including salaries, national insurance numbers, dates of birth and bank account details were also sent to a number of newspapers. Skelton was jailed for eight years in July 2015 for his actions.

Read more:

BBC News - Morrisons data leak: Supermarket liable for staff details breach

The Guardian - Morrisons found liable for staff data leak in landmark ruling

SC Magazine - Morrisons Supermarket held liable after employee leaks data

**Germany bans children’s smartwatches**

A German regulator has banned the sale of smartwatches aimed at children, describing them as spying devices. It had previously banned an internet-connected doll called, *My Friend Cayla*, for similar reasons.

Telecoms regulator, the *Federal Network Agency*, urged parents who had such watches to destroy them. One expert said the decision could be a "game-changer" for internet-connected devices. "Poorly secured smart devices often allow for privacy invasion. That is really concerning when it comes to kids’ GPS tracking watches - the very watches that are supposed to help keep them safe," said Ken Munro, a security expert at Pen Test Partners.

Read more:

BBC News - Germany bans children's smartwatches
Gizmodo - German Regulators Ban Smartwatches for Kids, Urge Parents to Destroy Them

Bundesnetzagentur (Press Release) - Bundesnetzagentur takes action against children's watches with "eavesdropping" function

Google faces UK suit over alleged snooping on iPhone users

A new consumer campaign called "Google You Owe Us" is launching a class action against Google over allegedly unlawfully harvesting the browsing histories of iPhone users without their permission.

A group of at least 5.4 million affected consumers could be owed hundreds of pounds each in compensation, according to Richard Lloyd, former Which? executive director and Government adviser, who is spearheading the action. The group alleges that Google's algorithms were able to bypass default iPhone privacy settings through the Safari web browser and collect individuals' data to target them with advertisements. The claimants allege that the breach took place between June 2011 and February 2012 and could have affected 5.4m people who could be eligible to make a claim against Google. A Google spokesperson said: "This is not new. We have defended similar cases before. We don't believe it has any merit and we will contest it."

Read more:

The Telegraph - Google could be forced to pay £2.7 billion in compensation to iPhone users

Financial Times - Google faces UK suit over alleged snooping on iPhone users

Mishcon de Reya - Google data breach case

Free Privacy Impact Assessment tool released by French DPA

The French Data Protection Authority (CNIL) has just released a free software tool relating to the conduct of a privacy impact assessment (PIA). The software is meant to guide the data controllers in building and demonstrating compliance to the GDPR. It helps to properly carry out a data protection impact assessment by facilitating the use of the PIA method developed by the CNIL. Although the download link is in French, the software is available in both English and French.

A video tutorial (in French only) is available here.

The software can be downloaded here.
Uber sued over massive data breach, EU taskforce created by Article 29 WP

After Uber revealed that it paid hackers $100,000 to keep quiet about stealing the personal information of 57 million customers and drivers, the company is now facing at least three potential class-action lawsuits and separate investigations by the attorneys general of New York, Missouri, Massachusetts, Connecticut, and Illinois. The company said it also has been in contact with the Federal Trade Commission.

According to the Washington Post, attorneys general Eric Schneiderman of New York, Lisa Madigan of Illinois, Maura Healey of Massachusetts and George Jepsen of Connecticut have launched investigations into the company.

Travis Kalanick, Uber’s co-founder and former chief executive, became aware of the breach a month after it occurred, according to Bloomberg. Instead of reporting the attack to regulators and victims last year, the company paid hackers $100,000 to delete the data and keep the security breach under wraps, Bloomberg reported.

In addition, the European Union privacy regulators have announced that they have established a taskforce on the Uber data breach case. This taskforce, led by the Dutch data protection authority, will be composed at this stage of representatives from the French, Italian, Spanish, Belgian and German data protection authorities as well as from the UK's ICO and will coordinate the national investigations on this issue.

Read more:

Washington Post - Uber is sued over massive data breach after paying hackers to keep quiet

Fortune - Uber's Cover-Up of Its Massive Data Breach May Lead to E.U. Investigations

Article 29 Working Party - Creation of a taskforce on the Uber data breach case

CNN - Uber's massive hack: What we know

UK’s ICO guide to the GDPR

The United Kingdom's Information Commissioner's Office has released their own guide to understand the GDPR. Although this guide does not provide any new information, it is nevertheless a useful reading since the guide is published by a regulator and provides some insight into what the regulators consider most important. It is also a useful read for those who are struggling to understand the concepts introduced by the GDPR.
Read more:

Information Commissioner's Office - Guide to the General Data Protection Regulation (GDPR)

Data Breach Hits Australia's Department of Social Services Credit Card System

According to The Guardian, The Australian Department of Social Services (the "DSS") has written to 8,500 current and former employees warning them their personal data held by a contractor has been breached. In letters sent in early November, the DSS alerted the employees to "a data compromise relating to staff profiles within the department's credit card management system prior to 2016."

Compromised data includes credit card information, employees' names, user names, work phone numbers, work emails, system passwords, Australian government services number, public service classification and organisation unit. The data related to the period 2004 to 2015.

Read more:

The Guardian - Data breach hits Department of Social Services credit card system

Other privacy-related news


Chicago Tribune - Analysis: Apple is sharing your face with apps. That's a new privacy worry

eWeek - Imgur Discloses Security Breach That Occurred in 2014

Wired - Anyone can hack MacOS High Sierra just by typing "root"

Wired - MacOS update accidentally undoes Apple's "root" bug patch

Tech Xplore - Princeton researchers spot website visits being watched

 Ars Technica - No, you're not being paranoid. Sites really are watching your every move

Engadget - The big stores that track your every online move
Future events

Complying with FAR and DFARS Cybersecurity Requirements

Format: Webinar  
Date: December 8, 2017  
Time: 12:00 PM - 1:30 PM ET  
Credits: 1.50 General CLE Credit Hours  
Panelists: Hilary Hageman, Jeffery Mitchell Chiow, Susan Booth Cassidy

This webinar will address the cybersecurity compliance obligations imposed on all government contractors by FAR 52.204-21 ("Basic Safeguarding of Covered Contractor Information Systems") and on defense contractors by DFARS 252.204-7012 ("Safeguarding Covered Defense Information and Cyber Incident Reporting"). The webinar will also discuss the legal consequences of non-compliance and also highlight some of the unique compliance obligations imposed on cloud services by DoD.

Read more here.

The Disaster Roadmap: Leveraging Funding and Best Practices

Format: Webinar  
Date: December 11, 2017  
Time: 1:00 PM - 2:30 PM ET  
Credits: 1.50 General CLE Credit Hours  
Panelists: Donna Boyce, Lisa Gavin, Wendy Huff Ellard  
Moderator: Erin Kathleen Capps

The 2017 hurricane season was one of the most brutal we've seen, reinforcing the important role that lawyers play in pre- and post-disaster preparation and assistance. This presentation will provide attorneys representing local governments and officials with an in-depth look at FEMA Hazard Mitigation Assistance (HMA) and Public Assistance (PA) programs.

Read more here.

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.