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

Burger King debuts Whopper ad that triggers Google Home devices and sparks privacy concerns

As marketers try to differentiate their TV spots from their competitors and make a connection with their audience, Burger King found a new way to do this: taking advantage of the Google Home device which may be sitting in the viewer's living rooms. In the ad, the friendly Burger King employee says "Ok Google, what is the Whopper burger?" and the Google home device would then react and immediately read the product description from Burger King's Wikipedia page. Privacy concerns about voice-activated speakers and the connected home have been on the rise lately as more companies are introducing "smart" connected devices.

Read more:

 Reuters - Burger King debuts Whopper ad that triggers Google Home devices

 Washington Post - Burger King thought it had a great idea. Instead, it ended up with a Whopper of a problem

 Engadget - Burger King wreaks havoc on Google Assistant with Whopper ad

Fine for UK Barrister who stored client files on home computer

Trump signs repeal of US broadband privacy rules

Civil rights lawyers plan to challenge New York's body-camera program

Article 29 Working Party issues draft guidelines on Data Protection Impact Assessments & high risk processing

March sees an uptick in health data breaches

FTC approves final consent order with digital advertising company charged with deceptively tracking consumers online and through mobile devices

China's data localization measures open for comment

FTC seeks comment on proposed changes to TRUSTE's COPPA safe harbor program

UK data breach could affect nearly 250,000 customers
home computer

A senior barrister who failed to keep clients’ sensitive personal information secure has been fined £1,000 by the UK Information Commissioner’s Office (ICO) which is the data protection authority in the UK.

According to the ICO, information belonging to up to 250 people, including vulnerable adults and children, was uploaded to the internet when the barrister’s husband updated software on the couple’s home computer. Some 725 unencrypted documents, which were created and stored on the computer, were temporarily uploaded to an internet directory as a back up during the software upgrade.

They were visible to an internet search engine and some of the documents could be easily accessed through a simple search.

Read more:
Information Commissioner’s Office - Fine for lawyer who stored client files on home computer

Trump signs repeal of US broadband privacy rules

On April 3rd, United States President Donald Trump has signed into law a bill that reverses Obama-era broadband privacy rules preventing Internet Service Providers (“ISP”) from selling a subscriber’s web browsing history and other personal information without permission.

The now-reversed law would have limited what ISPs like Comcast, Verizon, and AT&T could do with sensitive customer data like location, browsing history, and other personal information like Social Security numbers. Under the law, which would have been enacted at the end of 2017, ISPs were also required to strengthen protections against hackers and security breaches.

Read more:
Business Insider - Trump has signed the repeal of US broadband privacy rules
Forbes - The Nullification Of FCC's Broadband Privacy Rules: What It Really Means For Consumers

Civil rights lawyers plan to challenge New York’s body-camera program

Challenges by civil liberties lawyers and police unions could delay a pilot program for New York City police officers to wear body cameras. Lawyers see shortcomings
in policies on camera use, while unions representing captains, lieutenants and detectives want negotiations on supervisors' extra responsibilities under the program.

Read more:


Article 29 Working Party issues draft guidelines on Data Protection Impact Assessments & high risk processing

On 4th April 2017, the Article 29 Working Party (WP29) adopted draft guidelines on Data Protection Impact Assessments ("DPIAs"). DPIAs are mandated when the processing is "likely to result in a high risk to the rights and freedoms of natural persons". However, the WP recommends that they should be seen as a tool for accountability and could be used in somewhat wider situations as well: in the view of the WP29, conducting a DPIA will help organisations build compliance (at the outset) and demonstrate compliance at a later date.

Read more:

Article 29 Data Protection Working Party - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

March sees an uptick in health data breaches

The monthly breach report issued by Protenus last week outlining data breaches that occurred in the month of March concludes that there was an "uptick in the number of health data breach incidents." According to the report, there were 39 incidents last month that involved health information, compromising 1.5 million patient records. A whopping 44 percent of the incidents were the result of "insider threat," which includes both criminal (malicious) and accidental (honest) activity.

Read more:

Data Privacy + Security Insider - March Sees an Uptick in Health Data Breaches

FTC approves final consent order with digital advertising company charged with deceptively tracking consumers online and through mobile devices

Following a public comment period, the Federal Trade
Commission has approved a final settlement with a Redwood City, California company over charges that it deceived consumers by tracking them online and through their mobile applications even after consumers took steps to opt out of such tracking.

Turn Inc., which enables sellers to target digital advertisements to consumers, agreed in December 2016 to settle FTC charges that it misrepresented the extent to which it continued to track consumers even after they opted-out of such tracking. The company’s privacy policy told consumers they could block targeted advertising by using their web browser’s settings to block or limit cookies. The FTC’s complaint alleges, however, that Turn used unique identifiers to track tens of millions of Verizon Wireless customers, even after they blocked or deleted cookies from websites. The opt-out mechanism also only applied to mobile browsers.

Read more:
Federal Trade Commission - FTC Approves Final Consent Order with Online Company Charged with Deceptively Tracking Consumers Online and Through Mobile Devices

China’s data localization measures open for comment

On 11 April 2017 the Cyberspace Administration of China published a circular calling for comments on its draft Security Assessment for Personal Information and Important Data Transmitted Outside of the People’s Republic of China Measures (the Draft Export Review Measures). Public comments are open through 11 May 2017.

The main legislative purpose of the Draft Export Review Measures is to clarify the process and requirements relating to the data localisation provisions in the Cyber Security Law, one of the most controversial aspects of the law. While the Draft Export Review Measures do add a significant level of implementing detail as to the practicalities of compliance, we expect that for many multinational corporations with operations in, or doing business with, China, the nature of the clarifications do not go in the direction that they would have wanted. In particular, the Draft Export Review Measures include a significant expansion of the scope of the localization measure, potentially applying to all businesses collecting data in China.

Read more:
Hogan Lovells - China’s Data Localization Measures Open for Comment
**FTC seeks comment on proposed changes to TRUSTE’s COPPA safe harbor program**

The Federal Trade Commission is seeking comment on proposed changes to TRUSTe’s safe harbor program under the agency’s Children’s Online Privacy Protection Rule.

The FTC’s COPPA Rule includes a “safe harbor” provision designed to encourage increased industry self-regulation in this area. Under this provision, industry groups and others may ask the Commission to approve self-regulatory guidelines that implement the protections of the Rule. Companies that comply with the FTC-approved guidelines receive safe harbor from agency enforcement action under the Rule.

Read more:

Federal Trade Commission - FTC Seeks Comment on Proposed Changes to TRUSTE’s COPPA Safe Harbor Program

**UK data breach could affect nearly 250,000 customers**

As many as 250,000 Wonga customers are believed to be at risk after hackers attacked the firm’s database last week, exposing thousands of card numbers and sort codes. The payday loan company started contacting borrowers over the weekend after confirming cyber criminals had cracked the system - with access to names, addresses, phone numbers and bank account numbers. The Wonga breach is believed to be one of the biggest involving financial information to have hit a UK company.

Read more:

The Telegraph - Wonga data breach could affect nearly 250,000 customers’ bank details

**Future events**

**2017 Internet of Things National Institute**

May 10-11, 2017 - Washington, DC

Mark your calendars now to attend this conference to learn about this fast emerging, most transformative, and potentially most disruptive technology development in years!

**2017 ANNUAL MEETING SCITECH CLE PROGRAMS**
View Full SciTech Schedule of Events

THURSDAY, AUGUST 10

3:30 PM – 5:00 PM
Unblurring the Lines: Navigating the Complex Relationship between Technology, Music & Copyright Law

FRIDAY, AUGUST 11

2:00 PM - 3:30 PM
Immerse Yourself: Creative Expression through Augmented & Virtual Reality

3:45 PM – 5:00 PM

SATURDAY, AUGUST 12

2:00 PM – 3:30 PM
SHOWCASE PROGRAM
Cyber Risk Management: How Should Lawyers, Corporations and Governments Deal With Risk? (Co-sponsored with Cybersecurity Legal Task Force)

3:45 PM – 4:45 PM
Special Report on Cybersecurity