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

Uber settles FTC allegations that it made deceptive privacy and data security claims

Uber has agreed to implement a comprehensive privacy program and obtain regular, independent audits to settle Federal Trade Commission (FTC) charges that the ride-sharing company deceived consumers by failing to monitor employee access to consumer personal information and by failing to reasonably secure sensitive consumer data stored in the cloud. In its complaint, the FTC alleged that Uber failed to live up to its claims that it closely monitored employee access to consumer and driver data and that it deployed reasonable measures to secure the personal information it stored on the servers of a third-party cloud provider.

The FTC alleged that Uber did not take reasonable, low-cost measures that could have helped the company prevent data breaches. For example, according to FTC charges, Uber did not require engineers and programmers to use distinct access keys to access personal information stored in the cloud. Instead, according to the FTC, Uber allowed them to use a single key that gave them full administrative access to all the data, and did not require multi-factor authentication for accessing the data. In addition, Uber allegedly stored sensitive consumer information, including geo-location information, in plain readable text in database back-ups stored in the cloud.

"Uber failed consumers in two key ways: First by
misrepresenting the extent to which it monitored its employees' access to personal information about users and drivers, and second by misrepresenting that it took reasonable steps to secure that data," said FTC Acting Chairman Maureen K. Ohlhausen. "This case shows that, even if you're a fast growing company, you can't leave consumers behind: you must honor your privacy and security promises."

Under its agreement with the FTC, Uber is prohibited from misrepresenting how it monitors internal access to consumers' personal information and how it protects and secures that data. In addition, Uber is required to “implement a comprehensive privacy program that addresses privacy risks related to new and existing products and services and protects the privacy and confidentiality of personal information collected by the company”. It is also required “to obtain within 180 days, and every two years after that for the next 20 years, independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order”.

Read more:

Federal Trade Commission - Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims

TechCrunch - Uber agrees to 20 years of privacy audits to settle FTC data mishandling probe

EU-Canada sharing of passenger data struck down by European Court of Justice

The Court of Justice of the European Union (CJEU) has rejected a proposed deal between the EU and Canada for the sharing of passenger data on the basis of EU data protection and privacy rules. The CJEU ruled that while the transfer, retention and use of passenger data is allowed in general, the envisaged rules for handling sensitive personal data were "not limited to what is strictly necessary".

The EU and Canada negotiated an agreement on the transfer and processing of passenger data (Passenger Name Record or PNR), which was signed in 2014. The Council of the European Union requested the European Parliament's approval of the agreement, and the European Parliament decided to refer the matter to the Court of Justice in order to ascertain whether the envisaged agreement was compatible with EU law and, in particular, with provisions relating to the protection of personal data.

According to the CJEU's press release, this is the first time the CJEU has been called upon to give a ruling on the compatibility of a draft international agreement with the EU Charter of Fundamental Rights.
Since the EU has a PNR agreement with the United States and Australia, these agreements could potentially come under fire and face similar challenges in light of this ruling.

Read more:

Court of Justice of the European Union (Press Release) - The Court declares that the agreement envisaged between the European Union and Canada on the transfer of Passenger Name Record data may not be concluded in its current form.

Ontario Court of Appeal recognizes expectation of privacy in energy consumption data

On August 10, the Ontario Court of Appeal released its decision in R. v. Orlandis-Habsburgo, where it held that a utility sharing residents’ energy consumption data with police, which led to a search and criminal charges, violated their reasonable expectation of privacy. According to the Court, "information, like the energy consumption data, that is capable of supporting inferences that certain activities are going on inside a home can fall under the umbrella of a reasonable expectation of privacy, depending on a consideration of the totality of the circumstances."

Read more:

R. v. Orlandis-Habsburgo, 2017 ONCA 649

Torys - Ontario Court of Appeal recognizes expectation of privacy in energy consumption data

Updates to Sonos privacy policy stirs controversy

According to press reports, Sonos has emailed their customers to inform them of changes to its privacy policy, as it seemingly prepares to collect a range of data from its customers. However, it appears that the company is not allowing existing users to opt out of the new privacy policy, and has stated that unless customers accept the new policy, their devices may lose some of their functionality.

According to the revised privacy policy: "Certain categories of the data that we collect are absolutely necessary for your Sonos System to perform its basic functions in a secure way and you will not be able to opt out from this data collection, sharing and/or processing ("Functional Data")."

The collected data includes registration data (which includes the user's email address, location, language preference, Product serial number, IP address, and Sonos
account login information, but also system data which would include "Product type, controller device type, operating system of controller, software version information, content source (audio line in), signal input (for example, whether your TV outputs a specific audio signal such as Dolby to your Sonos system), information about Wi-Fi antennas, audio settings (such as equalization or stereo pair), Product orientation, room names you have assigned to your Sonos Product, whether your product has been tuned using Sonos Trueplay technology, and error information."

According to ZDNet, "a spokesperson for the home sound system maker told ZDNet that, "if a customer chooses not to acknowledge the privacy statement, the customer will not be able to update the software on their Sonos system, and over time the functionality of the product will decrease. The customer can choose to acknowledge the policy, or can accept that over time their product may cease to function," the spokesperson said."

Earlier this month, another controversy arose in relation to a proposed change of privacy policy of another company. Popular media player software maker Plex informed users via email about an updated privacy policy due to go into effect in September. The new policy was understood to remove users’ ability to opt out of data collection. This move quickly resulted in user backlash, with many subscribers concerned that their data would be shared or sold to third parties, or that Plex would be able to identify the media files housed in their library.

A subsequent blog post from Plex stated that its privacy policy was not clear enough and that the company had no interest in knowing what is in its users' libraries and had no intention to collect data to that effect. Plex further stated that it would soon make changes to its proposed privacy policy in order to address users' concerns.

Read more:

CSO Online - Sonos: Accept new privacy policy or devices may "cease to function"

ZDNet - Sonos says users must accept new privacy policy or devices may "cease to function"

Sonos - Privacy Statement

TechCrunch - Plex changes its new privacy policy after backlash, clarified it's not trying to see what's in your library

Plex - Privacy Policy Changes

Singapore to review personal data protection rules

Singapore's Personal Data Protection Commission (the
PDPC) is seeking views on its proposals, through a public consultation from 27 July to 21 September 2017, on two key areas – proposed enhanced framework for collection, use and disclosure of personal data, and proposed mandatory data breach notification. These proposals are part of the PDPC's review of Singapore's Personal Data Protection Act.

Under the proposals, it will be mandatory for organizations to inform customers of personal data breaches that pose any risk of impact or harm to the affected individual as soon as they are discovered. If an incident involves 500 or more individuals, organizations will need to notify the PDPC as soon as possible but no later than 72 hours after discovery of the breach.

Read more:

PDPC - First Public Consultation on Review of the PDPA

Russian data protection authority publishes privacy policy guidance

On 31 July, the Russian data protection authority, Roskomnadzor, issued guidance for data operators on the drafting of privacy policies to comply with Russian data protection law. Hogan Lovells' Chronicle of Data Protection reports that the Roskomnadzor generally considers it important for data operators to adopt a relatively detailed data processing policy so that data subjects are aware of all potential actions to be taken with their personal data, such as the purposes for processing and recipients of their personal data.

It is further reported that while these recommendations are generally in line with the principles stipulated in the Personal Data Law, certain recommendations contained in the guidance may need to be checked by companies, such as recommendations on the listing of all third parties receiving personal data along with details about the data transferred. Violations of the provisions of the Russian data protection law may result in a warning or a fine of up to RUB 30,000.

Read more:

Hogan Lovells’ Chronicle of Data Protection - Russian Data Protection Authority Publishes Privacy Policy Guidance

Data Breach at Massachusetts hospital: former employee inappropriately accessed data over last 14 years

A Massachusetts-based hospital, Tewksbury Hospital, recently discovered evidence of an incident of unauthorized electronic health record (EHR) access, potentially creating a data breach relating to protected
health information (PHI).

According to the official statement, "in April of this year, a former patient expressed concern that someone may have accessed their electronic medical record inappropriately. A review conducted in response to this complaint revealed that one hospital employee appeared to have accessed the former patient’s records without a good reason to do so. This discovery led to a broader review of the employee’s use of the electronic medical records system at Tewksbury Hospital. As a result of this review, it was determined that the employee appeared to have inappropriately accessed the records of a number of current and former Tewksbury Hospital patients.

Individuals who may be affected include people who were patients at Tewksbury Hospital from 2003 through May 2017. We have provided written notice to affected patients for whom the hospital has current contact information. We are also posting this substitute notice in a good faith attempt to notify affected individuals for whom we have insufficient or out-of-date contact information that precludes written notification, or to whom we are otherwise not able to provide written notice."

Read more:

Health IT Security - Tewksbury Hospital PHI Data Breach Threatens 1K Patients

Massachusetts Health and Human Services - Data Breach at Tewksbury Hospital

New Jersey's new Personal Information and Privacy Protection Act to limit retailers’ use of ID-embedded data

On July 21, 2017, New Jersey Governor Chris Christie signed into law the Personal Information and Privacy Protection Act. This legislation limits the purposes for which retail establishments may lawfully scan a person’s government-issued identification card, such as a driver’s license. It also limits the data that can be collected from such scanning and how these data can be retained and used.

The legislation was prompted by reports of retail stores misusing and improperly storing information obtained from scanned driver’s licenses, according to the bill’s sponsors. It is expected to take effect on October 1, 2017.

Read more:

Bloomberg BNA - N.J. Enacts Law to Limit Retailers’ Use of ID-Embedded Data

TalkTalk fined £100,000 for data breach of 21,000 customers
UK broadband provider TalkTalk has been fined £100,000 by the Information Commissioner’s Office (ICO) after the telecoms giant was found to have placed personal data from 21,000 customers at risk.

An ICO investigation found TalkTalk breached the Data Protection Act because it allowed staff to have access to large quantities of customers’ data. Its lack of adequate security measures left the data open to exploitation by rogue employees.

The breach came to light in September 2014 when TalkTalk started getting complaints from customers that they were receiving scam calls. The scammers pretended they were providing support for technical problems. They quoted customers’ addresses and TalkTalk account numbers. The investigation found the issue lay with a TalkTalk portal through which customer information could be accessed. One of the companies with access to the portal was Wipro, a multinational IT services company in India that resolved high level complaints and addressed network coverage problems on TalkTalk’s behalf.

According to the ICO, Wipro staff could log in to the portal from any internet-enabled device. No controls were put in place to restrict access to devices linked to Wipro. In addition, they could view large numbers of customer records (up to 500 customer records at a time) and export data. The ICO found this level of access was unjustifiably wide-ranging and put the data at risk.

Read more:

The Guardian - TalkTalk fined £100,000 for not protecting customers’ personal data

ICO - Personal data belonging to up to 21,000 TalkTalk customers could have been used for scams and fraud

Germany publishes English version of its national GDPR implementation act

The German Ministry of Interior affairs has published an English translation of the new Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG).

On 27 April 2017, the German Parliament passed the BDSG in order to make use of the opening clause provided for in the EU General Data Protection Regulation (GDPR). The full English version is accessible here.

Read more:

Hogan Lovells’ Chronicle of Data Protection - Germany Publishes English Version of its National GDPR Implementation Act

UK seeks data transfer pact with EU

BBC News reports that the UK government will seek "new arrangements" with the EU in order to facilitate the continued free flow of personal data.

According to the government's policy paper, the UK wants to explore a UK-EU model for exchanging and protecting personal data, which could build on the existing adequacy model, by providing sufficient stability for businesses, public authorities and individuals, and enabling the UK's Information Commissioner's Office (ICO) and partner EU regulators to maintain effective regulatory cooperation and dialogue for the benefit of those living and working in the UK and the EU after the UK's withdrawal.

Read more:
BBC - Brexit: UK seeks data transfer pact with EU

India's Supreme Court rules privacy a 'fundamental right' in landmark case

A nine-judge bench of the Supreme Court of India ruled on August 24th that privacy is a fundamental right and that “informational privacy is a facet of the right to privacy,” a decision that could have an impact on a pending lawsuit over social media data sharing.

The ruling sets the stage for a final resolution of an ongoing litigation over WhatsApp’s sharing of subscriber data with its parent Facebook, which is slated for a court hearing on September 6. Other online companies, including Twitter, are also likely to face closer regulatory scrutiny in the future and potentially be exposed to a flood of litigation over corporate data-sharing practices, according to Bloomberg BNA.

Read more:
Bloomberg BNA - Ahead of WhatsApp-Facebook Ruling, India Holds Privacy Fundamental
CNN - India Supreme Court rules privacy a ‘fundamental right’ in landmark case

Future events

Managing Cyber-security Due Diligence in Technology M&A Transactions
This CLE webinar is intended to provide transactional attorneys and in-house counsel with an overview of the tools needed to effectively manage cyber-security due diligence within the context of high technology merger and acquisition (M&A) transactions. Leading practitioners will discuss how to identify, evaluate and manage an acquisition target's cyber-security strengths and weaknesses throughout and beyond the deal-making process.

Discussion topics will include analysis of a hypothetical target's internal cyber-security program; compliance with applicable cyber-security and privacy law; and international cyber-security risk mitigation strategies.

Read more here.

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

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.

Read more here.

Legal Process Outsourcing: Is the Technology Right for Your Firm?

Format: Webinar
Date: September 19, 2017
Time: 1:00 PM - 2:30 PM ET
Credits: 1.50 General CLE Credit Hours
Panelists: Byron G Buck, Erin Frances Giglia, Laurie G
Rowen and Wilton Hathaway Strickland

**Moderator:** Mark Ross

With the growing shift in technology and the need to better serve clients, many firms are turning to legal process outsourcing. Much of the work is transferred to external vendors either domestically or overseas. Using external resources is extremely beneficial for smaller firms since it frees up talent and is widely known for improving efficiency. The ABA's Model Rule 1.1 promotes technological competence, but are there unknown issues that attorneys should consider when contracting with other attorneys or legal staff outside of their firm? This webinar will explain the risks and benefits of outsourcing your legal work.

Read more [here](#).

You are currently subscribed to the American Bar Association's E-Privacy Law Committee mailing list. Your e-mail address will only be used within the ABA and its entities. We do not sell or rent e-mail addresses to anyone outside the ABA.

[Update your profile](#) | [Unsubscribe](#) | [Privacy Policy](#)

**American Bar Association:** 321 North Clark Street | Chicago, IL 60654 | 800-285-2221

Copyright © 2017 ABA, All Rights Reserved.