Foreword

According to a report from Krebs on Security, the data breach suffered by fast food chain restaurant Wendy's could be much worse than the high-profile Target and Home Depot breaches.

The report quoted B. Dan Berger, CEO at the National Association of Federal Credit Unions, who stated that many credit unions "saw a huge increase in debit card fraud in the few weeks before the Wendy's breach became public" and that the bulk of the fraud activity was tied to customers who had patronized Wendy's locations less than a month prior to the breach.

One credit union CEO indicated that losses could be “five to ten times worse” than with Target or Home Depot and further said that, as of January 2016, his organization was already halfway to reaching a normal year's worth of fraud.

As a reminder, Target agreed to a $39.4 million settlement with financial institutions late last year following fraudulent charges made in the wake of its 2013 breach affecting about 40 million debit and credit cards. Likewise, Home Depot agreed to a $19.5 million settlement following its massive 2014 data breach affecting 56 million debit and credit cards. We could potentially be looking at much higher numbers for the Wendy's data breach.

In addition, according to Courthouse News, a class-action complaint has been filed in Orlando federal court alleging that the restaurant chain "employed inadequate safety measures and failed to quickly send notice to customers."

This latest incident serves as a reminder on how important it is for companies to double down on the security of their information systems.

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.
Tinder accused of breaching EU rules

The Norwegian Consumer Council has filed an official complaint with the Norwegian Consumer Ombudsman (Forbrukerombudet) against Tinder, alleging that Tinder's terms and conditions breaches Norwegian and EU consumer and privacy laws.

According to the complaint, accepting Tinder's terms and conditions grants Tinder "an irrevocable, perpetual, non-exclusive, transferable, sub-licensable, fully paid-up, worldwide right and license to (i) use, copy, store, perform, display, reproduce, record, play, adapt, modify and distribute the content, (ii) prepare derivative works of the content or incorporate the content into other works, and (iii) grant and authorize sublicenses of the foregoing in any media now known or hereafter created. […] This permission granted to Tinder by the user is far-reaching and would appear to be infinite. It includes all forms of storage and processing of information, including the sharing of information with partners ("affiliates" and "licensees")."

Even though Tinder has no European operation or representation, the complaint further alleges that Norwegian law is applicable since "the service has been adapted for the Norwegian market in that the language used in the actual application is Norwegian for Norwegian users and that the service is marketed in Norwegian on the Apple App Store."

See also:
Fortune - Tinder Is in Trouble Over Its 'Unfair' User Terms
Norwegian Consumer Council - NCC files complaint against Tinder for breaching European law

Right to be forgotten: Google to use geolocalisation

On March 4, 2016, Google announced that it will use geolocation signals (like IP addresses) to restrict access to delisted URL on all Google search engine domains, including google.com, when accessed from the country of the person requesting the removal. Previously, delisting was only carried out on European extensions of the search engine and not when searches are made from "google.com" or other non-European extensions.
That old approach was criticized by the French data protection authority, the CNIL, who considered that delisting should be carried out on all extensions of the search engine. Would geolocation be sufficient to appease the CNIL? The CNIL has already indicated that, "contrary to Google's statements, applying delisting to all of the extensions does not curtail freedom of expression insofar as it does not entail any deletion of content from the Internet. At a physical person's request, it simply removes any links to website pages from the list of search results generated by running a search on the person's first name and surname. These pages can still be accessed when the search is performed using other terms." As a result, the CNIL has issued a €100,000 fine against Google.

Source:
Google Europe Blog - Adapting our approach to the European right to be forgotten
CNIL - Right to be delisted: the CNIL Restricted Committee imposes a €100,000 fine on Google

EU-US Privacy Shield under fire

A coalition of civil society groups has sent a letter to European policy makers reviewing the EU-US Privacy Shield to rethink the framework. Privacy International, the Electronic Frontier Foundation, American Civil Liberties Union (ACLU), and Amnesty International USA are just some of the 27 groups who signed the letter. The letter was sent to Ms. Isabelle Falque-Pierrotin (Chairman of the Article 29 Working Party), MEP Claude Moraes (Chair of the Committee on Civil Liberties, Justice, and Home Affairs) and HE Pieter de Gooijer (Ambassador and Permanent Representative of the Netherlands to the EU).

According to the letter, "without more substantial reforms to ensure protection for fundamental rights of individuals on both sides of the Atlantic, the Privacy Shield will put users at risk, undermine trust in the digital economy, and perpetuate the human rights violations that are already occurring as a result of surveillance programs and other activities. The Article 29 Working Party thoughtfully outlined four key conditions for an agreement to meet the standards of European legislation and guarantee the protection of human rights in intelligence activity, including clarity of law, use of human rights standards, incorporation of independent oversight, and availability of effective remedy. Unfortunately, the Privacy Shield manifestly fails to provide for these objectives."

This is not the first time that the Privacy Shield has been openly criticized. Sheila Fitzpatrick, worldwide data governance counsel and chief privacy officer at storage firm NetApp, believes that it contains only "cosmetic" changes and there is much work to do if it will not have to be renegotiated, according to an article on Computing. John Whelan, a partner at law firm A&L Goodbody, said in the Irish Independent that the Privacy
Shield is "unlikely to survive for long" and would not pass the Court of Justice of the European Union.

Source:
Transatlantic coalition of civil society groups - Privacy Shield is not enough, must return to negotiating tables

Facebook Appears to Address Plugin Privacy Concerns

On March 17, 2016, Facebook argued for the dismissal of a case alleging that the social media giant tracked user internet activity after having logged out of their Facebook accounts.

The case is specifically about Facebook’s “like” and “share” plugins that allow websites outside of Facebook to leverage Facebook’s open graph to drive greater traffic. The plug-in has been questioned for its privacy ramifications from the beginning. Facebook argues that the plaintiff's have not suffered a particularized harm and have not stated a claim upon which relief may be granted.

Read more:
Law 360 - Facebook Says Users Don't Show Harm In $15B Tracking MDL

FCC Announces Rule Making on Broadband Consumer Privacy

On March 10, 2016, the Federal Communications Commission (FCC) announced the Notice of Proposed Rulemaking on Broadband Consumer Privacy. The new rules will seek to emphasize consumer choice, transparency, and security.

The factsheet accompanying the notice further outlines the goals of the rulemaking and specifically notes the exclusion of topics including the privacy practices of specific companies and government surveillance or encryption. The promulgated rules are set to be released any day now.

Read more:
Data Law Insights - Privacy & Cybersecurity Weekly News Update
Safe & Sound - Proposed Broadband Consumer Privacy Rules Circulated to Federal Communications Commission

New Jersey SC Rule 6-0 Approving the
Constitutionality of Roving Wiretaps

In early March, the New Jersey Supreme Court approved law enforcement’s use of roving wiretaps on suspect phone. These orders allow law enforcement to tap an alternate phone used by suspects without an additional warrant when the suspect intentionally switches phones to avoid surveillance. In reaching this decision, the court found that an “inherent exigency circumstance” was created when the suspect purposefully switches devices. However, the court did build in a small privacy protection. The holding requires law enforcement to notify the wiretap judge within 48 hours of the switch and obtain authorization to continue monitoring.

Read more:
Data Law Insights - Privacy & Cybersecurity Weekly News Update
Law 360 - NJ Justices Say Roving Wiretaps Don't Violate Privacy Rights

Growing Number of Top Officials Siding with Apple

As the legal battle between the FBI and Apple is put on hold, a number of top government officials have come out supporting Apple. Having a change of heart, General Michael Hayden, a former head of the NSA and CIA, gave his support for Apple. While he stated that he wants to “side with the bureau,” he is unable to support the bureau because “this is not a one-and-done.” Overall, General Hayden commented that intelligence agencies should focus on the volumes data they are able to get and glean information from because content is going to be increasingly elusive.

Former DHS Security Michael Chertoff indicated that what the FBI is demanding of Apple would be akin to asking them "to create a biological weapon". These sentiments were echoed by Mike McConnell (former director of National Intelligence and Navy vice Admiral) and Nuala O’Connor (former Chief Privacy Officer of DHS) who also advocated the strong encryption is fundamental to our national security, especially with the growing Internet of Things.

Finally, FTC Commissioner Terrell McSweeney announced she opposed a law forcing tech companies to provide encryption keys to law enforcement. In her comments, she emphasized the dangers of legislating vulnerabilities into devices.

Upcoming events
Practical Tips to Avoid Cyber Risks and Understand the Legal Liability of “Smart” Devices

25 billion "smart" devices are estimated to be wirelessly connected to, and communicating with, each other by the year 2020, raising serious legal and liability issues. This "Internet of Things" (IoT) is transforming our economy, our culture and our legal system. This program will provide an overview of the pending transformation, address the risks of non-traditional mobile devices such as medical devices and smart watches, including privacy and security, and explore how to manage the risks in our Internet of Things world with both traditional and non-traditional mobile devices.

Format: Webinar
Date: May 3, 2016
Time: 1:00 PM - 2:30 PM ET
Panelists: Meghan Elizabeth Butler Richard J Johnson Stephen S Wu, Rebecca A Nielsen
Credits: 1.50 General CLE Credit Hours

Register here for the webinar.

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.
Thank you for your continued interest in this list. A summary of your discussion list subscriptions, including ST-EPRIVACY, can be found at https://shop.americanbar.org/ebus/myABA/CommunicationPreferences.aspx. This new List Subscription Page allows you to manage your lists - unsubscribe from existing or join others. If you have any issues you may either contact the list owner via email: ST-EPRIVACY-request@mail.americanbar.org, or the ABA Service Center at phone: 1-800-285-2221 or email: service@americanbar.org.

The purpose of this discussion site is to enable ABA members to share and exchange their personal views on topics and issues of importance to the legal profession. All comments that appear are solely those of the individual, and do not reflect ABA positions or policy. The ABA endorses no comments made herein.