Attorney Advertising

Robinson+Cole

March 26, 2015

Data Privacy and Security Insider

DATA BREACH

Target agrees to settle data breach class action suit for $10 million

Judge Paul Magnuson, who is presiding over the Target multi-district class action litigation in Minnesota, preliminarily approved the parties' proposed settlement of the litigation involving the infamous breach affecting up to 110 million individuals during the holidays in 2013 for $10 million.

The Agreement requires Target to pay $10 million into an escrow account to pay consumer claims of up to $10,000 each if they can document losses, up to $6.75 million in attorney's fees and the remainder to go to the rest of the class who can't document their losses. Class members can submit their claims through the mail or online.

Target also agreed to:

- pay all administrative costs;
- appoint a chief information security officer;
- maintain a written information security program;
- develop a process to monitor and respond to security events; and
- provide security training to its employees.

Although it is understandable that Target wanted to stop the bleeding from the litigation, the plaintiffs in the Target case were never required to prove Article III standing to show that they had actually suffered harm as a result of the security breach, which unfortunately provides class action lawyers an incentive to continue to bring class action litigation against any company that suffers a data breach. Based on recent history, that list will only get longer and data breach class action litigation is here to stay.

– Linn Foster Freedman

DATA PRIVACY

Amazon gets FAA approval to use drones for test fly delivery

In February 2015, the Federal Aviation Administration (FAA) released a framework for how it plans to oversee the operation of small drones weighing 55 pounds or less. Now, on March 20, 2015, the FAA has come to an agreement with Amazon.com Inc. (Amazon), and issued it an online retailer experimental airworthiness certificate, to permit it to test fly delivery drones for research and development purposes. With this certificate, Amazon can now conduct test drone flights at 400 feet or below during daylight hours, as long as the drone remains in visual line-of-sight of the operator. Each Amazon drone operator must also have a private pilot's certificate and current medical certification. Amazon will also be required to submit monthly reports to the FAA that provide information on the number of flights carried out, pilot

duty time per flight, unusual modifications, and other flight data. The test fly delivery drones are set to hit the skies in rural Washington State.

Amazon general counsel, Stephanie Burns, said in a public statement, “The outdoor-testing operations we seek in our petition for exemption [under the February 2015 framework] are a necessary step towards realizing the consumer benefits of Prime Air, as well as a step in unlocking the enormous potential of [drones]. Aerial delivery is poised to make goods available to consumers in a manner that is more environmentally friendly than current surface delivery methods, while improving overall safety of the transportation system.” Look out above.

– Kathryn M. Sylvia

Data privacy, security and breach notification bill passes through House subcommittee

A closely watched bipartisan national data privacy, security, and breach notification bill cleared a House subcommittee yesterday, sending it to the full House Energy and Commerce Committee for review. There have been many similar bills introduced over the years to attempt to establish one clear standard for data privacy and breach notification, to replace the 47 different state laws in place now. None of them have been successful yet.

This legislation aims to set a national standard for data privacy, security and breach notification by requiring companies to report cyber intrusions, share information about cyber hackings, strengthen consumer protection and apply a uniform data breach notification standard. The subcommittee added several amendments to the bill, including one requiring the FTC to educate small businesses about data security.

There continues to be criticism of some aspects of the bill, but in this environment when massive data breaches are occurring every day, the timing for setting a national standard may be riper than in the past. Many predict this bill will die like the ones before it, even though it is needed now more than ever, but we will continue to watch it as it winds through the system.

– Linn Foster Freedman

Toysmart Pt. Deux

An auction of RadioShack assets which concluded this week included the names and physical addresses of 65 million customers and email addresses of 13 million customers. The auction result and transfer of assets is still subject to bankruptcy court approval.

Many states, including Texas and New York, have promised to take legal action to stop the transfer, because it violates the company's privacy policy. RadioShack's March 2015 privacy policy stated "We will not sell or rent your personally identifiable information to anyone at any time."

Other companies, such as AT&T have also objected to the sale.

http://www.pcworld.com/article/2901028/radioshack-puts-customers-personal-data-up-for-sale-in-bankruptcy-auction.html

– Kathleen Porter

Federal student privacy law in flux

In recent months, the White House and members of Congress have called for an overhaul of the forty-year old Family Educational Rights and Privacy Act (FERPA) ((20 U.S.C. § 1232g; 34 CFR Part 99), which safeguards the privacy of students’ educational records.

Originally enacted in 1974, FERPA applies only to federal funded elementary, secondary and postsecondary educational agencies and institutions. Thus, FERPA does not extend to restrict private companies from disclosing student information. Given the nature of education today, there are many private companies providing services to students and their parents, including college planning consultants, career services providers, college testing and application companies and other third party vendors. Right now, a student and a parent have to review applicable state law and the privacy policies of these private companies to determine how the student's personal records will be protected.

In addition to the White House, members of the Senate and the House have talked about introducing new student-data-privacy legislation. The pending House version, written by Representatives Jared Polis (D-CO) and Luke Messer (R-IN) is expected to closely align with President Obama's policy initiatives.

Specific areas of focus for improving existing federal law include expanding the definition of "education record" to include digital data and metadata, broadening FERPA's applicability to education technology vendors, adopting data security standards and providing for a tiered enforcement structure and regulating the sharing or sale of student data to third parties for purposes unrelated to education.

In the interim, the Privacy Forum and the Software and Information Industry Association the private sector has published a set of voluntary standards to protect K-12 student privacy. To date more than 125 signatory companies, including Apple and Microsoft have pledged to follow the standards.

Some twenty states have also taken action to fill what has been perceived as a gap in federal student privacy law and regulation, with a majority of states having introduced bills that address student privacy in recent years. Last fall, California adopted the Student Online Personal Information Protection Act (SOPIPA) which restricts the use of students' educational data by third-party vendors.

Institutions and vendors active in the education industry likely will want to actively monitor federal and applicable state privacy laws and regulations (and, importantly, the direction in which any new legislation may be trending), and consider refining their practices as necessary to remain compliant with the evolving privacy landscape.

– Robert Barbieri + Kathleen Porter

ENFORCEMENT + LITIGATION

FTC v. LabMD administrative proceeding postponed

The saga between the FTC and LabMD will not be resolved anytime soon. The case has been at a standstill since last May, and late last week, the administrative law judge postponed the proceeding until May 5th.

The case stems from an alleged data breach of LabMD's patient information in 2010. The FTC investigated the incident and filed an administrative complaint against LabMD alleging that its security practices violated Section 5 of the FTC Act. LabMD has consistently maintained that the FTC has overextended its authority under Section 5. LabMD was forced to unwind its business as a result of the investigation.

Fireworks have exploded in the case as LabMD alleges that Tiversa, the company that provided the information to the FTC on the alleged data breach, basically took the data from LabMD's server, while Tiversa has responded that the data was found outside LabMD's server. LabMD has a previous employee lined up to testify after the witness was granted immunity from the Department of Justice.

The case will be exciting to follow on multiple levels--the challenge to FTC's regulatory authority, the testimony about how the data was obtained and given to the FTC, and how the investigation destroyed a company who fought back. We will be on the edge of our seats and will keep you updated as the proceeding gets underway in May.

– Linn Foster Freedman

Class action filed against Rag & Bone for collection of customer information during credit card

transactions

Lead plaintiff, Bernadine Griffiths, and other Rag & Bone Industries LLC (Rag & Bone) customers filed a class action in California state court against high-end clothing retailer for asking customers for identifying information during credit card transactions. The complaint alleges that Rag & Bones intentionally engaged in a pattern of unlawful business tactics through its company "information capture policy." This policy requires that Rag & Bone cashiers ask for and record personally identifiable information from customers at the time of credit card transactions in violation of California's Song-Beverly Credit Card Act (the Act). The Act prohibits this exact conduct; companies are not permitted to ask for personally identifiable information during a credit card transaction.

The complaint stated, "As part of Rag & Bone's information capture policy, and in conjunction with the credit card sales transaction, plaintiff was asked for [her] address, telephone number, and e-mail address." The class consists of consumers whose information was collected after March 20, 2014; it does not include those consumers who provided their information for shipping purposes, delivery or special orders. The class action demands up to $1,000 per violation. We'll stay on top of the this as it proceeds.

– Kathryn M. Sylvia

Solicitor General supports proposed class action against Spokeo

The U.S. Solicitor General has filed an amicus brief asking the U.S. Supreme Court to reject Spokeo's appeal of a lower court decision allowing a proposed class action to move forward because Spokeo allegedly published false information about the named plaintiff in violation of the Fair Credit Reporting Act (FCRA). He further alleged that Spokeo compiles false information from many sources, prepares reports and sells the information, in violation of the FCRA.

The case hinges on whether the named plaintiff has Article III standing to sue under the FCRA if he can't show actual damages. Spokeo's stance is supported by eBay, Facebook, Google and Yahoo. They argue that if the Court allows the proposed class to go forward without the requirement to show actual harm, the floodgates will open for class action litigation for no injury violations of the Telephone Consumer Protection Act, the Video Privacy Protection Act and other statutes.

The Solicitor General argued that the "public dissemination of inaccurate personal information" is concrete harm that should satisfy the harm element of Article III standing.

– Linn Foster Freedman

Judge refuses to toss out TCPA class action against Guess

U.S. District Judge John A. Houston denied Guess, Inc.'s (Guess) Motion to Dismiss plaintiff, Farideh Haghayeghi's, class action claims that Guess sent text messages in violation of the Telephone Consumer Protection Act (TCPA). Guess argued that Haghayeghi's allegations were just "a patchwork recital" of TCPA regulations, and that the complaint had no facts to substantiate a TCPA claim. However, on March 24, 2015, Judge Houston found that Haghayeghi's January 2014 complaint indeed contained sufficient factual allegations. Judge Houston further supported Haghayeghi's complaint, stating that she specifically alleged that Guess did not obtain prior express consent before sending telemarketing text messages.

Judge Houston said, "The class, as currently defined is suspect as it requires a finding that defendant sent unauthorized text messages to determine who is a class member. However, the court finds it more appropriate to address the issue in a motion for class certification." The litigation will therefore continue, as Judge Houston found "that the complaint sufficiently articulates the substance of plaintiff's claims and permits defendant to obtain more specific details through the discovery process." TCPA actions are becoming less of a burden for plaintiffs and more costly for defendants; the lesson –know what the TCPA requires and adhere to those standards.

– Kathryn M. Sylvia

Apple and Twitter fail to escape App Store privacy class action

On March 24, 2015, U.S. District Court Judge Jon S. Tigar determined that the plaintiffs in a privacy class action against Apple, Inc. (Apple) and Twitter Inc. (Twitter) sufficiently alleged that they relied on Apple's advertisements boasting the security of its mobile devices, and that Twitter and other mobile app developers invaded their privacy by collecting their contacts from their mobile devices without consumer knowledge. Attorney for the plaintiffs stated, "It's been a very hard-fought case, and we're glad that we're finally able to move into discovery phase. It's a good day for privacy, and for users of Apple products and the Internet in general."

Judge Tigar applied a six-part test commonly used in tobacco advertisement cases to determine whether Apple's misrepresentations met the criteria necessary for the class action to proceed. Judge Tigar determined that the plaintiffs can indeed make these fraud-based allegations based on extensive, long-term advertising campaigns without necessarily identifying specific statements made by Apple that were misleading.

Twitter and other mobile app developers asked Judge Tigar to dismiss the allegations that they invaded consumers' privacy by accessing contacts on Apple devices, but the Court rejected Twitter's plea and concluded that while consumers may have been aware that certain mobile apps would require access to their personal contacts in order to function properly, these plaintiffs did not know that the information would be used in unauthorized ways. The key to complying with privacy laws and steering clear of the courtroom seems to be transparency with the consumer.

– Kathryn M. Sylvia

SOCIAL MEDIA

Social media analytics firm raises $130 million

Dataminr, a venture backed data analytics firm that analyzes Twitter posts and other public sources to provide real time information to news sources, investment banks and the government, recently announced that it has raised an additional $130M, adding to its initial funding of $180M.

Founded in 2009 by two Yale roommates, Dataminr started offering its services to the investment world, providing real-time information to assist with investment decisions. It has expanded to news organizations and governments which need real time information about potential disasters.

Monetizing social media data has exploded in recent years, which underscores the value of the data. This trend will only continue as new and advanced technology is developed to mine and analyze datasets to repurpose it in the market. We will continue to report on significant deals and funding in the data analytics and technology spaces.

– Linn Foster Freedman

CYBERSECURITY

Cybersecurity: corporate counsel's role

The Indiana University Maurer School of Law recently released "The Emergence of Cybersecurity Law," an industry whitepaper discussing the role of corporate counsel on preparing for and responding to cyberattacks.

The whitepaper underscores the necessity of corporate counsel shifting from the historical role of post-security incident response to one where they are leading the company's effort to put in place tools, training and response strategies before the occurrence of a security incident. This proactive approach, according to the whitepaper, will improve the company's response and prevent further escalation of the incident. Corporate counsel's role includes coordinating the creation of a cybersecurity plan for the

organization, working with IT, risk management, the board and senior management. The whitepaper highlights 10 points of focus for corporate counsel, including working with legal counsel familiar with a cybersecurity program, training employees on incident avoidance and breach response and looking at potential insurance coverage to manage risks.

– Kathleen Porter

To get more thoughtful and timely discussions of legal news and perspectives on various issues relating to data privacy and security, subscribe to our *Data Privacy and Security Insider Blog*.

Check it out at www.dataprivacyandsecurityinsider.com and subscribe by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share the blog with anyone you think would find it useful.

Linn F. Freedman
One Financial Plaza, Suite 1430
Providence, RI 02903
401.709.3353
lfreedman@rc.com

Kathryn M. Sylvia
One Financial Plaza, Suite 1430
Providence, RI 02903
401.709.3357
ksylvia@rc.com
