Robinson+Cole

April 2, 2015

Data Privacy and Security Insider

DATA BREACH

Multiple class action lawsuits filed against Premera Blue Cross for data breach Days following Premera

Days following Premera Blue Cross's public announcement that it had experienced a data breach affecting approximately 11 million, it has been sued five times (as of the time of this writing) in proposed class action lawsuits in federal district court in Washington. On top of that, it is facing investigations from at least three states—Washington, Alaska and Oregon, and it is rumored that insurance commissioners in other states are considering joining the investigation ranks. The Governor of Alaska has also ordered state agencies to review their security standards and those of state business associates. The Premera breach reportedly affected approximately 700,000 Alaskans, including employees of the State of Alaska. The information breached included the individuals' names, dates of birth, Social Security numbers, email addresses, home addresses and bank account information from 2002 to 2015.

The crux of the proposed class action lawsuits is that Premera waited too long to inform customers of the breach, which may have commenced last May but was discovered in January.

Unfortunately for Premera, on April 18, 2014, just a few weeks before the initial intrusion, the Office of the Inspector General informed Premera that its security procedures were lacking following an audit. The plaintiffs' attorneys have used this information to allege in the complaints that Premera failed to fix basic security issues and had sufficient time to do so to prevent the ongoing access to sensitive data.

We expect additional lawsuits to be filed against Premera as we have seen in other major data breach cases, and we will watch them closely and report on developments as they occur. Stay tuned…

– Linn Foster Freedman

ENFORCEMENT + LITIGATION

U.S. Supreme Court holds that ankle bracelet monitoring is a form of search and seizure

On Monday, the U.S. Supreme Court in *Grady v. North Carolina* vacated the judgment of the Supreme Court of North Carolina upholding the use of a GPS monitor on a recidivist offender. The statute authorizing the program explained that the purpose of the GPS monitor was "for time correlated and continuous tracking of the geographic location" of the offender in order to report his missteps.

The Supreme Court held that the program was designed to obtain information by physically intruding on an individual and, thus, constitutes a Fourth Amendment search. This decision is consistent with

Supreme Court precedent in recent years. In 2012, the Court held that the installation and monitoring of a GPS tracking device on a suspected criminal's vehicle was a search within the meaning of the Fourth Amendment. The following year, the Court held that using a drug-sniffing dog to investigate around a suspect's front porch was a search because police "had gathered information by physically entering and occupying the curtilage of the house to engage in conduct not explicitly or implicitly permitted by the homeowner."

The Court refused to decide whether the program was unconstitutional. Rather, the Court remanded the case to the North Carolina courts to make findings as to whether the state's monitoring program was reasonable.

– Kathleen E. Dion

Walgreen Settles Prescription Robocall Suit for $11 million

Walgreen Co. this week settled a putative class action law suit alleging that it violated the Telephone Consumer Protection Act (TCPA) for $11 million. The plaintiffs alleged that Walgreen violated TCPA when it placed unsolicited prerecorded prescription refill reminders to customers on the cell phones.

Walgreen defended the calls by stating that because the plaintiffs provided their cell phone numbers when refilling their prescriptions previously, that constituted "express written consent" required by TCPA, and also that it fell under an exemption of the TCPA and was allowed to call the cell phones for an "emergency purpose" of furthering the health and safety of its customers.

After Walgreen was unsuccessful in getting the claims tossed, initial discovery ensued and the parties agreed to settle.

In addition to paying $11 million to the proposed class for approved claims submitted (estimated at $15 a piece), Walgreen has agreed to implement procedures to confirm that customers consent to receive automated calls on their mobile phone numbers in their customer profiles, and also to provide customers with an option to opt in or opt out of receiving prerecorded calls to their cell phones.

The lessons learned in all of these TCPA class action suits? TCPA continues to be a hot topic for plaintiffs lawyers because of the availability of a private right of action and automatic damages of $500 per call and $1500 for a willful violation of the TCPA. Companies looking to market and/or contact customers via text messages and/or prerecorded calls should be wary and ensure compliance with the TCPA before launching the campaign.

– Linn Foster Freedman

LabMD files Motion to Exclude Exhibits as it gears up for May 5th hearing with FTC

The litigation between LabMD and the FTC is not mellowing.

Last week, LabMD filed a Motion to Exclude the FTC's admission of all Tiversa documents during the FTC administrative hearing scheduled for May 5th. LabMD argued that the FTC subpoenaed Tiversa in September of 2013, and Tiversa withheld responsive information from the subpoena, which to date, has never been produced. The FTC subpoena requested "all documents related to LabMD" and when Tiversa failed to produce the documents, the FTC did not enforce the subpoena. Accordingly, since some documents were never produced, LabMD argues that no documents should be allowed to be used during the hearing. We will be watching that proceeding closely.

– Linn Foster Freedman

HIPAA

Beware medical records subpoenas: Connecticut Supreme Court issues opinion on negligence for noncompliance with HIPAA standards

Health care providers and their medical records custodians constantly find themselves under pressure to release medical records immediately upon receipt of a subpoena. However, regardless of the subpoena or the pesky insistence of the requesting attorney, with the recent ruling by the Connecticut Supreme Court in *Byrne v. Avery Ctr.*, 314 Conn. 433 (2014), health care providers' responses to requests for medical records must be compliant with the Health Insurance Portability and Accountability Act (HIPAA) more than ever. To adhere to HIPAA regulations, health care providers must first receive "satisfactory assurances" that the person whose medical records are requested received notice of the request. While most subpoenas include some type of notice language, the Court outlined that to truly show "satisfactory assurances" the requesting attorney must have provided:

1. Written notice to the affected individual;

2. Sufficient information for the individual to raise an objection; and

3. Time for the individual to raise an objection or confirm that there are no objections or that all objections have been resolved.

The requesting attorney may also provide "satisfactory assurances" that it has secured a protective order prior to the issuance of the subpoena. The Court said in its opinion that it is not enough for a subpoena to include a statement that a protective order WILL be filed or for it to include DRAFT language for a protective order. The appropriate protective order must be FILED with the court. Remember, there could also be other state laws that apply to protected health information and state laws that are even more restrictive than HIPAA when it comes to sensitive health information such as mental health treatment or sexually transmitted diseases.

Under this new opinion from the Connecticut Supreme Court, health care providers in Connecticut who fail to comply with HIPAA may be subject to patient lawsuits and possible state damages for negligence and emotional distress, in addition to a potential federal investigation for HIPAA violations.

– Kathryn M. Sylvia

DATA PRIVACY

NJ first state to restrict access to car recording device data

Did you know that your car has a recording device that records the speed, direction, and location of your vehicle while you are driving it, as well as your steering, braking, seat belt use and erratic driver behavior?

On March 26, 2015, the New Jersey General Assembly unanimously approved the first (to our knowledge) state statute that limits access to data recorded by motor vehicles. The Act provides that no person, except the owner of a motor vehicle, may "retrieve, obtain or use data recorded, stored or transmitted" from automobile recording devices unless: 1) it is with the owner's consent; 2) it is subject to a search warrant or other administrative order; 3) it is for the purpose of improving motor vehicle safety; 4) it is to a dealer or for the vehicle's repair; 5) it is by emergency response personnel; or 6) it is pursuant to a discovery request or order in a civil action.

The Act prohibits further disclosure of the data unless it is de-identified or it is with the owner's written consent. The Act has strict provisions relating to the prohibition of altering or preventing access to the data and violation of the Act is punishable with a $5,000 fine for each offense.

– Linn Foster Freedman

Privacy rights group speaks out against FAA's proposed framework on commercial use of drones

On March 31, 2015, the Electronic Privacy Information Center (EPIC) filed a petition against the Federal Aviation Administration's (FAA) proposed rule on commercial drone use, in the D.C. Circuit. EPIC believes that the FAA did not create privacy safeguards in its proposed rule as mandated by Congress. EPIC explains in its petition that Congress requires the FAA to create a "comprehensive plan" for private drone use in the FAA Modernization and Reform Act of 2012. EPIC asks that the D.C. Circuit find that the FAA's failure to propose drone privacy rules in its rule unlawful.

While the FAA did claim that it would make privacy issues a top concern, when it released the proposed rule in February 2015, the FAA did not address privacy issues stating that such issues were "beyond the scope of this rule making." However, to fill this gap, President Obama did release a memorandum ordering federal agencies to comply with privacy and civil liberties as well as an order for the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) to develop best practices for commercial drone use. For now EPIC's complaint still stands. No best practices have been developed by the NTIA and more commercial drones have begun flying in the air.

– Kathryn M. Sylvia

CYBERSECURITY

Spam emails sent from fridge in botnet attack

The Internet of Things allows consumers to program and monitor all sorts of equipment, devices and appliances, including smart meters, ovens, TVs and refrigerators. It is well known that most of these devices that are connected to the internet do not have any security protections, as they have been designed solely for consumer convenience.

The type and amount of data collected on these devices in your home should be a consideration--particularly after security company Proofpoint has discovered a botnet attack that occurred between December 23rd and January 6th. This botnet attack hijacked devices, including routers, multimedia centers, TVs and at least one refrigerator to send over 750,000 spam emails. Proofpoint reported that over 25% of the emails were sent from devices that weren't computers or mobile devices, and it is the first known case of a refrigerator being used in a cyber attack. And to think that all this time we have been worried about cyber attacks from China, North Korea and Russia. Buyer beware: that smart appliance could be a cyber hacker.

– Linn Foster Freedman

Recent research suggests medical device interoperability poses cybersecurity risks

While improved interoperability between medical devices will certainly lead to better care management and more efficient, effective medical treatment, new cybersecurity issues for hospitals and health care organizations are also on the horizon. A recent, and ongoing, study conducted by the University of Michigan School for Computer Science and Engineering found that "the more devices are interoperable, the more complex these systems become, and complexity is what a hacker wants." Securing medical devices before hospitals and health care organizations add these devices to their networks will provide a more secure method and better protect patient's personal and medical information. Unsecured medical devices can be an easy gateway for a hacker to access hospitals' IT and financial management systems.

Additionally, a recent survey of 526 nurses between January 7 and January 16, 2015, found that improved medical device interoperability may save the health care industry billions of dollars each year

and could reduce the number of medical errors. To read the full survey, click here. The lesson here is to ensure that medical devices are secure and untouchable by third parties before potentially allowing unauthorized access to droves of personal and financial information.

– Kathryn M. Sylvia

---

e-DISCOVERY

People matter: cultural challenges in cross border e-discovery

As U.S. litigators and U.S. courts begin to gain some level of comfort with advanced e-discovery practices, new challenges have emerged in the form of cross-border discovery. While most U.S. attorneys are aware that there are challenges associated with collecting data from individuals and entities in Europe and Asia, they tend to focus primarily on the legal and technical challenges presented by the data privacy and security laws in those regions.

A recent article in Law Technology News by Chris DeMarco, entitled "Culture Shock: The Human Side of E-Discovery," reminds us that people are still an essential part of the e-discovery process, particularly in the pre-collection stages, and that cultural differences can also impact the success of an e-discovery project abroad. Based on an interview with Ashley Smith, managing director at Navigant Consulting, Inc., who has conducted e-discovery projects throughout the world, the article provides a reminder of the importance of the human elements associated with e-discovery, such as strategy sessions and custodian interviews, and offers suggestions to manage cultural expectations to ensure a productive project, and ultimately to ensure that the process is defensible. Of particular importance is partnering with local counsel to gain a deeper understanding of the social norms and customs.

Although these considerations might seem far afield from the bits and bytes we've come to associate with e-discovery, the process is only as good as the people…no matter what side of the ocean they are on.

– Andrea Donovan Napp

SOCIAL MEDIA

Pinterest's value hits $11 billion

Social media company Pinterest announced that it is worth $11 billion after its latest funding round of $367 million. Pinterest, founded in 2010, which calls itself a "visual bookmarking tool" helps its customers discover and save their ideas, but has recently moved into the advertising world through its acquisition of Kosei, Inc., which matches advertisers to specific consumers. This valuation confirms that investing in social media companies continues to be strong in the market as the digital world continues to expand.

— Linn Foster Freedman

CHILDREN'S PRIVACY

FTC updates COPPA FAQs related to educational context

On March 24, 2015, the Federal Trade Commission (FTC) updated the Children's Online Privacy Protection Act (COPPA) Frequently Asked Questions (FAQs) to better address the intersection of COPPA regulations and schools. Specifically, the FTC updated FAQs M.1, M.4, and M.5. FAQ M.6 was deleted from the list because the FTC felt that the issue of a student's use of an online social network in school was addressed by FAQs M.1 and M.2. To review the FTC's summary of changes, click here.

– Kathryn M. Sylvia

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
