November 5, 2015

DATA BREACH

Mental Health Center Hacked

Not-for-profit mental health center Emergence Health Network, located in El Paso, Texas, has announced that its computer servers were compromised "through an unauthorized internet connection" from as far back as 2012.

The center discovered the compromise in August when it "became aware of strange activity on one of our computers."

A forensic analysis revealed that an unauthorized person gained access to the system through an Internet connection, and the first "unapproved access of the server may have happened back in 2012."

The intruder had access to over 11,000 mental health patients' names, addresses, dates of birth, Social Security numbers, case numbers and information that the individuals sought services at the center. The center stated "we are confident that no medical records were contained within the server."

Nonetheless, the disclosure of the sensitive mental health records was reported to the Office for Civil Rights and the affected patients.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

LifeLock Agrees to Pay FTC $116M

We previously reported that the FTC had filed suit against LifeLock alleging that it had violated a previous settlement with the FTC regarding false advertising and was in contempt.

The previous settlement ended with LifeLock paying $12 million and agreeing to refrain from falsely advertising its products and services.

The FTC has asked the court to stay the request for a contempt order to finalize the proposed settlement, which may include a payment of up to $116 million, which has been set aside by the company.

— Linn Foster Freedman

Background Check Companies to Pay $13 Million for FCRA Violations

General Information Services (GIS) and e-Background-checks.com Inc. (e-Background) agreed to pay $13 million in restitution and fines to settle their violations of the Fair Credit Reporting Act (FCRA) charged by the Consumer Financial Protection Bureau (CFPB). The CFPB charged GIS and e-Background with failure to ensure that the background checks they produced to potential employers had accurate information about the job applicants. GIS and e-Background will pay $10.5 million (or $1,000 per affected job applicant) and will also pay $2.5 million in civil penalties. CFPB Director Richard Corday said, "[GIS and e-Background] failed to take basic steps to provide accurate background screening reports to employers about job applicants [. . .] we are holding two of the largest companies in this market accountable for cleaning up the quality of their reports."

The erroneous background checks were conducted between July 2011 and December 2014, and affected over 11,000 people. There was no written policy regarding research of people with common names, no middle name requirement, and no audit processes in place to ensure accuracy of reports. Many reports contained inaccurate criminal records, crimes that had actually been expunged or dismissed and misdemeanors reported as felonies. In addition to these fines, policies and processes will be updated (and implemented) and an independent consultant will review all policies and procedures to ensure appropriate measures are in place.

— Kathryn M. Rattigan

Western Union to Pay $8.5 Million for Alleged TCPA Violations

Western Union will pay $8.5 million to settle alleged violations of the Telephone Consumer Protection Act (TCPA) when it sent consumers unsolicited text messages advertising an "opt-in" for receiving periodic automated updates concerning Western Union's money and wire transfer services. Lead plaintiff, Jason Douglas, first received a text message from Western Union advertising its services in 2009. Douglas alleged in his complaint that Western Union used equipment capable of storing and randomly generating telephone numbers to send out these text messages. And while the text messages did ask the consumer to "opt-in" to receive future text messages, Douglas alleged in his complaint that he never consented to receive the first telemarketing text message.

Based on Western Union's documentation, there are more than 800,000 potential class members who will be notified via e-mail and postcard, and thereby directed to a settlement website or a telephone line where they can make claims to their portion of the settlement. An individual will be considered a class member if they live in the U.S. and received at least one unsolicited text message between March 2012 and the date of the final approval of this agreement by Western Union. However, if all potential class members make a claim, each member would only receive $10.32. And this $10.32 amount is almost double the next highest amount-per-class-member from any court-approved TCPA settlement. Is that really enough?

— Kathryn M. Rattigan

DATA PRIVACY

SEC OKs Crowdfunding for Start-ups

On Friday, October 30, the Securities and Exchange Commission (SEC), by a vote of *3-1*, adopted rules designed to implement a 2012 law that allows start-ups to use crowd funding to generate investments in their companies.

Starting in the middle of 2016, businesses will be able to legally sell stock online to investors. This will assist companies to use the widespread power of the Internet to generate capital, while allowing investors to invest early in the next blockbuster idea or service.

However, the SEC is warning investors that fraud is a concern, as online scams are rampant. The SEC rules require that the crowdfunding securities offerings can only be made through brokerage firms or Internet funding portals that are registered with the SEC. Further, there will be caps on how much investors can invest, which is based on annual income. The cap will be $100,000.

But sit tight for now. The rules don't go into effect until sometime next year, and the SEC hasn't given us an idea of when that will be. Nonetheless, it is an exciting development for start-ups and investors alike, and we will let you know when the SEC rules are issued.

— Linn Foster Freedman

"Hell No Barbie" Campaign Against the New Interactive Doll with Artificial Intelligence

Well folks, it's that time of year again, the time of year where the latest and greatest toys hit the shelves just in time for the Christmas shopping season. This year, one of the most controversial toys to hit the shelves will be *Hello Barbie*, which is an interactive doll with artificial intelligence capable of having a real conversation. A real conversation? Yes, *Hello Barbie* will use voice recognition technology and a microphone to transmit the child's dialogue to an Internet server for interpretation, which will then elicit a tailored, prerecorded response from *Hello Barbie* to the child. A little bit creepy? I'll say.

Because of *Hello Barbie's* conversational abilities, the privacy group, Campaign for a Commercial-Free Childhood (CCFC) plans to warn parents and children about this new toy through its "Hell No Barbie" campaign. The campaign was launched this week on social media and on the CCFC website. CCFC's executive director, Josh Golin, says, "This is kind of the perfect storm of a bad toy." The CCFC argues that *Hello Barbie's* WiFi connection combined with its microphone could potentially act as an intermediary to pass personal information about children to companies for marketing research, hackers could access children's dialogue, and children's conversations will be monitored by Mattel, Inc. (Mattel) to improve and update the *Hello Barbie* artificial intelligence system.

However, Mattel says that *Hello Barbie* will NOT be used for any kind of marketing or advertising campaign and that Mattel has "integrated a variety of privacy and security measures into *Hello Barbie's* hardware and software." Additionally, parents will have the capability to listen to their children's recorded conversations and delete anything that they do not want on the *Hello Barbie* server. However, the CCFC doesn't like that either. The CCFC says that "children need that space to explore and to work out their own feelings without feeling like they're being surveilled by their parents or by a corporation."

Besides these potential privacy concerns, this *Barbie* will be sitting on the shelves for a mere $74.99 (while a typical *Barbie* only costs around $20). So before we start discussing the privacy concerns, let's see how many of these things go flying off the shelves.

Watch the video demonstration of *Hello Barbie's* capabilities here.

— Kathryn M. Rattigan

The Rules of Preservation: "Reasonable Steps" under Amended Rule 37(e)

Amended Federal Rule of Civil Procedure 37(e), which takes effect on December 1, 2015, authorizes courts to impose sanctions if electronically stored information (ESI) is lost because a party failed to take "reasonable steps to preserve it." Although "reasonable steps" is a phrase that will surely be litigated and ultimately defined by the courts, the Advisory Committee Notes provide some insight into the intent behind the revision, which is a wholesale replacement of the old Rule 37(e), and outline factors that a court may consider in analyzing whether a party's preservation efforts satisfy the new standard.

The Advisory Committee Notes are clear that "reasonable steps" is not synonymous with perfection, expressly recognizing what litigants have known for years—that the "ever-increasing volume of electronically stored information" and the "multitude of devices that generate such information" have made "perfection in preserving all relevant" ESI nearly "impossible."

Although the Advisory Committee Notes are not as unequivocal on what is reasonable, they do provide a road map of the factors a court might consider in assessing whether a party's preservation efforts rise to the level of "reasonable steps." These factors include:

- The sophistication of the parties with regard to litigation. A multinational corporation or serial litigant will likely be held to a higher standard than an individual plaintiff.
- A party's awareness of the risk of loss. The Advisory Committee Notes indicate that a party should not be held accountable for a loss outside of its control but suggest that courts may consider the party's knowledge of the risk of loss and whether adequate steps were taken to guard against such risk.
- Proportionality. Acknowledging that "aggressive preservation" carries a hefty price tag, the Advisory Committee Notes recommend considering a party's financial and human resources and acknowledge that less costly methods of preservation may be acceptable if they are "substantially as effective" as more costly forms.

— Andrea Donovan Napp

CYBERSECURITY

NAIC Cybersecurity Task Force Adopts Cybersecurity Bill of Rights for Insurance Consumers

On October 14, the National Association of Insurance Commissioners (NAIC) Cybersecurity (EX) Task Force released an updated draft of its Cybersecurity Bill of Rights. The bill, which updates a prior draft published for comment in July 2015, details certain rights of insurance consumers in connection with protection of personal information and responses to data breaches by insurers and agents. Specifically, insurance consumers have the right to:

1. Know the types of personal information collected and stored by insurers, agents or their vendors,
2. Expect insurers to make their privacy policies available on their website and in hard copy, if requested,
3. Expect insurers to prevent unauthorized access to personal information,
4. Receive notice from insurers in the event of a data breach through first class mail or email, sent within 60 days of discovery,
5. Receive 1 year of identity theft protection paid for by the insurer involved in a data breach,
6. In the event of identity theft, be aware of the measures available to protect their credit and prevent

contact from debt collectors.

This draft scales back some of the protections contained in the July 2015 draft published for comment, which included specific references to consumer protections under the Fair Credit Report Act and HIPAA. While the bill would not have binding effect, there has been concern voiced in the industry about whether the bill implies that consumers have greater rights than provided for under individual state laws. The bill will now go before the NAIC Executive (EX) Committee for approval in November.

— Benjamin C. Jensen

WEEKLY PRIVACY TIP #8

How Teachers Can Assist Students to Be Safe Online

It is scary to read the headlines that kids become victims of crimes, some of them horrific, because of online activity. Kids are naive and susceptible to online predators. Parents must be vigilant in educating their children about online activity and teachers can reinforce lessons learned at home to help kids stay safe.

How can teachers help?

The FTC has great resources for educators to share with students. And they are free! (I know how all of you teachers out there spend your own money on your students—this one is free!)

The resources include topics on cyber bullying, downloading apps, and protecting personal information and teaches these lessons through videos and games that are designed for kids of different ages.

There are educator resources available to elementary, middle school, high school and community educators. They are easy to follow and great tools for teachers to use, to help their students.

Check them out on the FTC website.

— Linn Foster Freedman

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog 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 this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.
