November 12, 2015

DATA BREACH

Dow Jones & Co. Notifies 3,500 of Data Breach

Dow Jones & Co. has notified 3,500 of its customers that their information was accessed by an unauthorized individual in a data breach that spanned from August 2012 through July 2015.

The unauthorized access, through malware, exposed the names, addresses, email addresses, telephone numbers, and credit card information of 3,500 subscribers, including subscribers to *The Wall Street Journal*.

The assumption is that the targeted attack was for the purpose of sending fraudulent solicitations and phishing attacks to these individuals.

Nonetheless, Dow Jones has notified the individuals and is offering identity protection services to those affected by the intrusion.

— Linn Foster Freedman

ENFORCEMENT+LITIGATION

CT AG Slams Hartford Hospital and EMC for Loss of Laptop

True to his word, the Connecticut Attorney General (AG) has aggressively entered the data privacy and security enforcement arena with a $90,000 settlement with Hartford Hospital and EMC.

The AG has agreed to a payment of $90,000 from Hartford Hospital and EMC over an incident in which an unencrypted laptop, which contained personal information of 8,883 patients, was stolen from an EMC employee's home.

The employee was working on a quality improvement project for Hartford Hospital and had downloaded the information on the laptop.

In announcing the settlement, AG Jepson stated, "All healthcare providers and any contractors who work with healthcare providers should pay close attention to [data privacy] responsibilities and review their internal controls and policies to ensure that they're doing all they possibly can to comply with the law and

to keep this information safe."

In addition to paying the penalty, Hartford Hospital agreed to implement additional policies and training protocols. EMC has also agreed to maintain policies requiring encryption of removable media and portable devices.

This is another example of why it is imperative for hospitals and health care providers, and their business associates and subcontractors, to ensure that no protected health information is downloaded to an unencrypted laptop or portable device and a reminder to use encryption technology to protect health information.

— Linn Foster Freedman

Company's Use of GPS to Track Employee Did Not Violate Collective Bargaining Agreement

On November 2, 2015, the National Labor Relations Board (NLRB) released an advisory letter stating that Shore Point Distribution Co. (Shore Point), an alcoholic beverage distributor in New Jersey, did not violate labor laws by failing to negotiate with its employees' union before installing a GPS tracking device on an employee's company truck. Beginning in March of this year, Shore Point believed that the employee was stealing time while on his work routes, and after using a GPS tracking device and a private investigator to follow him, fired the employee for his actions. The NLRB said in its letter that, the collective bargaining agreement contains rules against stealing time and requirements that company drivers follow federal regulations related to accurate accounting of their time. Additionally, the NLRB said in its letter that because the union permits the company's practice of hiring a private investigator for purpose of monitoring employees suspected of stealing time, and *the GPS was only used in conjunction* with the private investigator's observations, the collective bargaining agreement was not violated. The GPS was only installed on the employee's vehicle on the days when the private investigator was following the employee, and was used as a backup method in case the private investigator lost visual sight of the employee and his vehicle.

— Kathryn M. Rattigan

FCC Settles Data Security Enforcement Action with Cox

In what had been touted as the first data security enforcement action with a cable operator, the Federal Communications Commission (FCC) has agreed to settle for $595,000 an enforcement action following a data breach with Cox Communications. The settlement was announced by the FCC last week.

The settlement involves a data breach from 2014 when intruders broke into Cox Communication's IT systems and accessed the personal information of millions of its customers. The intruder, dubbed "Eviljolie" was allegedly a member of the Lizard hacker group.

Using social engineering, Eviljolie was able to access customers' information and change passwords and accounts.

Cox has agreed to notify all affected customers and provide credit monitoring to those affected by the intrusion. It has also agreed to implement a comprehensive compliance plan, including a written information security program, which will be monitored by the FCC for seven years. This requirement is strikingly similar to consent decrees required by the FTC in its data security enforcement actions.

The lesson? All industries should be focusing on a written information program to protect the personal information of employees and consumers and employee training to thwart social engineering and phishing expeditions.

— Linn Foster Freedman

Google Seeks Dismissal or Stay of Email Scanning Litigation

Google has recently asked a California federal court to dismiss a proposed class action alleging that the company's practice of scanning Gmail users' e-mail for marketing data violates federal and state privacy laws, primarily the Electronic Communications Privacy Act (ECPA).

The crux of Google's motion is that users of the company's highly popular Gmail consent to the practice when they sign up for the free email service. While plaintiffs have yet to respond to the motion, they are likely to focus on the fact that the proposed class consists of non-Gmail users who never agreed to Google's terms of service. In its motion papers, Google addresses this point by noting that the proposed class only seeks injunctive relief, which it argues requires a showing of ongoing ECPA violations without the injunction. Google claims plaintiffs cannot meet the burden because communications where one party consents (i.e., the Gmail user that consented to the scanning practice) is, as a matter of law, not an unlawful interception under the ECPA.

Alternatively, Google seeks a stay of the litigation pending the Supreme Court's decision in *Spokeo, Inc. v. Robins*, No-13-01339, a case where the highest court will decide whether Congress has the power, by authorizing a private right of action based on a violation of federal statute, to confer standing on a plaintiff to pursue a claim even where no concrete harm has been suffered. Argument in the Spokeo matter is scheduled for November 2, 2015, with a decision expected no later than June 2016.

The case is *Daniel Matera v. Google Inc.* case number 5:15-cv-04062 in the United States District Court for the Northern District of California.

— Brian J. Wheelin

Supreme Court Denies Cert in Case Involving Cell Location Privacy Rights

On July 31, 2015, Quartavious Davis petitioned for *certiorari* in *Davis v. United States*, No. 15-146, asking (1) whether the acquisition of a cell phone user's location data from his cellular service provider constitutes a search under the Fourth Amendment and (2) if it is a search, whether the search requires a warrant.

In previous posts, we explained how a number of courts have considered whether the Fourth Amendment requires law enforcement to obtain a warrant to access cell phone geographic location information. In May of this year, the Eleventh Circuit Court of Appeals held that Mr. Davis had no reasonable expectation of privacy in his cell phone location records and, even if there were such an expectation, a warrantless search was still reasonable.

The Supreme Court denied Mr. Davis's petition on November 9, 2015, but it remains an important issue. As noted in the Brief of Amici Curiae Electronic Frontier Foundation, the Brennan Center for Justice at NYU School of Law, Center for Democracy & Technology, The Constitution Project and the National Association of Criminal Defense Lawyers in Support of Petitioner, there has been a dramatic increase in the number of cell phones and cell sites in the last 20 years. Additionally, the number of law enforcement

requests for location information is increasing, and Courts continue to be faced with resolving whether a warrant is required.

— Kathleen E. Dion

Pharmacy Settles TCPA Class Action for $15 Million for Unsolicited Fax Ads

PharMerica settled a Telephone Consumer Protection Act (TCPA) class action initiated by a group of nursing homes over allegations that the pharmacy inundated the nursing homes with unsolicited fax advertisements in violation of the TCPA. The class action was filed back in October 2013 after PharMerica sent out over 100 fax-blasts to advertise the "PharMerica Education Symposium & Exhibition Series" in Orlando, Florida. The fax advertisements went to at least 11,000 nursing home facilities. Now, PharMerica has agreed to pay $15 million to settle these allegations and will also implement a new training program to educate staff members about TCPA compliance. To date, 409 valid claims have been submitted for a piece of the settlement, and in the end, none of the settlement will revert back to PharmMerica. This shows us that businesses not only need to comply with TCPA regulations when it comes to telephone calls and text messages, but consumers are still seeking damages for unwanted fax advertisements as well.

— Kathryn M. Rattigan

E-DISCOVERY

How to Use the Rule 26(f) Conference to Avoid Data Dumps

Back in the days of paper discovery—when productions came in bankers' boxes and document reviews involved paper cuts—litigators would attempt to try to gain a tactical advantage by "burying" opponents under mountains of paper. The modern version of this litigation tactic is the "data dump." Data dumps involve responding to discovery requests or subpoenas by unnecessarily transmitting large quantities of electronically stored information (ESI), much of which is irrelevant, often without any explanation or organization. This practice is even more problematic than its old-school counterpart because of the time and cost associated with e-discovery. If ESI lacks organization—that is, if it is produced in a confusing array of formats or in obsolete formats without proper indexing, or contains file types different from what was requested—the data may be impossible to electronically organize, search, or review. Structured data, like the data from databases, can be dumped in an unstructured, unusable state without the program they were created with or detailed information on how they were created and stored. Moreover, massive quantities of data drive up the costs of review, are time consuming, and may impede litigation efforts by obscuring the real issues.

While the temptation to drown adversaries in an avalanche of useless data can be high, courts have uniformly disapproved of such gamesmanship. For example, in *SEC v. Collins & Aikman Corp*., No. 07 Civ. 2419, 2009 WL 94311 (S.D.N.Y. Jan. 13, 2009), the Securities and Exchange Commission (SEC) dumped 1.7 million records, comprising 10.6 million pages, on the defendant and told it to search them for relevant materials, asserting that it did not have a way to collect documents relating specifically to the subjects relevant to the case. In reviewing the SEC's actions, the court stated that Rule 34 of the Federal Rules of Civil Procedure prohibits "simply dumping large quantities of unrequested materials onto the discovering party along with the items actually sought." Id. at *4. The court also found that expecting the defendant to do the plaintiff's work, which would have taken a substantial amount of time and money, constituted "undue hardship by any definition." Id. at *5. In the end, the court ordered the SEC to perform its e-discovery duties in accordance with the rules. To read the full article and get more tips on how to avoid data dumps, click here.

— Kelly Frye Barnett

CHILDREN'S PRIVACY

Parental Consent by Selfie?

As a general rule, the Children's Online Privacy Protection Act (COPPA) requires operators of websites (including mobile apps) directed to children under 13 to obtain verifiable parental consent before collecting personal information from those users. COPPA sets forth a nonexhaustive list of acceptable methods for obtaining parental consent. For example, operators can ask parents to sign and return a consent form by U.S. mail, fax, or electronic scan, or they can direct parents to call a toll-free telephone number staffed by trained personnel, among other methods. Needless to say, many of the currently sanctioned methods are impractical and ill-suited to the pace of technology today, particularly mobile usage habits.

One company, Riyo, Inc., is currently seeking approval from the Federal Trade Commission (FTC) for a two-step facial recognition process that would require a parent to take a picture of his or her photo identification and then take a "selfie" using a smartphone or computer camera. The parent would then send the two pictures to the operator for review. If the pictures were determined to be authentic and to match, parental consent would be deemed verified.

The FTC recently announced that it is delaying its decision on the proposed method until November 18, 2015. While the proposal would appear to offer a practical alternative to some of the more outmoded methods of obtaining parental consent, it comes with its own privacy concerns. How would the photos be analyzed and with whom would they be shared? Where would the photos be stored and what security measures would be in place to prevent improper disclosure of the information submitted by parents?

The Riyo proposal is another good example of the challenges and tensions in the world of digital privacy. It will be interesting to monitor the FTC's response as an indicator of the agency's adaptability (or caution) in the fast-changing digital marketplace.

— Christopher J. Librandi

PRIVACY TIP #9

Destroying Prescription Information

Have you ever noticed how much of your personal information is included on a prescription bottle and its packaging? Take a look next time you pick up a prescription at the pharmacy.

The outer packaging may include your name, address, date of birth, insurance information, physician name, prescription information and refill information.

The same is true for the prescription bottle.

Most people casually discard both in the trash, while properly destroying other pieces of paper that include the same information, because they don't recognize the extent of the personal information that is included.

The tip this week is to shred the outer packaging and the label of all prescription bottles because they contain detailed personal information about you that can be accessible by others. Protect this information just as you would any other piece of paper or electronic information with sensitive details about your health.

Be aware of when your personal information is included on things you don't expect such as prescription bottles and packaging. Don't forget to do the same for your children.

— 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.
