Robinson+Cole

April 9, 2015

Data Privacy and Security Insider

ENFORCEMENT + LITIGATION

PF Chang's continues its success in thwarting data breach class action lawsuits

We have been closely watching the class action suits against PF Chang's (and other retailers) relating to the bistro's data breach last year. In December, a federal district court in Illinois dismissed a proposed class action against PF Chang's because the plaintiffs were unable to show that they had suffered actual harm as a result of the data breach and therefore, did not have standing to pursue the claims. The plaintiffs appealed the dismissal to the Seventh Circuit Court of Appeals, and on March 20, 2015, PF Chang's requested that the Seventh Circuit affirm the lower court's dismissal.

Last week, a Washington federal judge followed suit and dismissed another proposed class action against PF Chang's in Washington federal court because the plaintiff was unable to show.

We will continue to follow data breach class action suits as they wind their way through the court system and keep you fully informed of their progress.

– Linn Foster Freedman

FCC urged to clarify TCPA regulations for sake of companies and consumers

"We can't paint all legitimate companies with the brush that every call from a private company is a form of harassment. It is time for the [Federal Communications Commission (FCC)] to act to provide clear rules of the road that will benefit everyone, and that means acting on [Telephone Consumer Protection Act (TCPA)] petitions before us." Federal Communications Commissioner, Michael O'Reilly, said on April 2, 2015, during his remarks to the Association of National Advertisers, that the FCC must act quickly on the pile of petitions related to the TCPA to clarify everything from the definition of an automatic telephone dialing system to a company's liability for making telemarketing calls to reassigned cell phone numbers. With the uncertainty surrounding TCPA regulations right now, telecommunication companies are experiencing high risks in litigation from the influx of class actions. O'Reilly said that while he does not support those companies that "hound[ ] consumers with incessant or harassing calls," he seeks to clarify the regulations so that health care providers can more easily contact patients with relevant information and allow banks to notify consumers in fraudulent situations. O'Reilly explained, "[C]ompanies are trying to provide a useful service, and if we make it too burdensome or costly for them to do so, then they won't make calls. It's that simple." Let's see how the FCC responds to those pending petitions. We'll keep you updated.

– Kathryn M. Sylvia

Data breach class action suit against Horizon Blue Cross dismissed

Late last week, a federal court judge in New Jersey dismissed a putative class action lawsuit against Horizon Blue Cross for a data breach involving two unencrypted laptops that were lost in 2013. The case alleged that close to 840,000 individuals' information was breached, including names, addresses, dates of birth, health information and Social Security numbers.

The plaintiffs alleged that Horizon failed to put appropriate security measures in place following a data breach in 2008, and it said it would implement security measures following a government investigation of that breach, which involved 300,000 individuals' information. However, it failed to implement the measures, which contributed to the data breach in 2013 involving the unencrypted laptops. Nonetheless, the judge dismissed the case because the plaintiffs "have not alleged an 'economic injury' sufficient for standing."

– Linn Foster Freedman

Microsoft versus the Federal Government; Round Three

Microsoft Corporation's (Microsoft U.S.) reply brief is due this week in its appeal of The District Court for the Southern District of New York's order to comply with the U.S. government's warrant requiring the turnover of a customer's emails stored in Ireland by its Irish subsidiary. The warrant was issued pursuant to the U.S. Stored Communications Act, which permits the government to request disclosure of a U.S. company's overseas records.

To date, Microsoft has refused to turn over the stored emails, on the grounds that the U.S. government has no grounds to order a company to execute a search warrant on private emails stored overseas. Several Microsoft competitors, as well as industry and business groups, the European Union and the Irish governments, have filed amicus briefs in support of Microsoft's position in this case. The Second Circuit Court of Appeals will hear arguments on the case later this Spring.

At issue is whether the U.S. federal government can require Microsoft U.S. to execute a "warrant" to seize private emails of customers from an overseas server owned by an affiliate corporation, and return them to the U.S. for viewing by prosecutors. Microsoft and its supporters argue that the private emails in question are protected by Irish and European Union laws, and any request to turn them over should be decided by a court in those jurisdictions rather than a U.S. court. Alternatively, Ireland argues that the emails should be disclosed to the U.S. only upon approval of a request to the Irish government pursuant to the long standing Mutual Legal Assistance Treaty (MLAT) between the U.S. and Ireland. The MLAT sets forth a process by which the U.S. government could request the information for law enforcement purposes, in this case, the prosecution of a suspected drug trafficker, and the Irish Government would consider the request and whether to grant it.

If Microsoft should lose this case, the impact could affect cloud computing arrangements globally, and U.S. owned or controlled cloud providers specifically. Individuals, foreign companies and governments might hesitate to store data in the cloud of a U.S. owned or controlled company for fear it is not secure. Germany has already required that any company providing cloud services to the German government must certify that the stored data will not be subject to seizure by a foreign government.

See In the matter of a Warrant to Search a certain e-mail account controlled and maintained by Microsoft Corporation 14-2985-cv. Microsoft Corporation, Appellant, v. United States of America, Appellee.

– Kathleen M. Porter

CYBERSECURITY

IBM identifies cybercriminals' increased use of Dyre Wolf to steal millions

IBM researchers reported late last week that they have identified an increase in the use of Drye Wolf malware which has contributed to the loss of millions of dollars from victim companies. Drye Wolf allows the intruders to spread malware spam through a mass mailing of victims' contacts lists.

According to the IBM researchers, the cybercriminals' recent use of Dyre Wolf "shows a brazen twist from the once-simple Dyre malware by adding sophisticated social engineering tactics likely to circumvent two-factor authentication. In recent incidents, organizations have lost between $500,000 and $1.5 million to attackers." It appears that the attackers are " targeting organizations that frequently conduct wire transfers with large sums of money" through phishing expeditions. When the expedition is complete, the intruders have obtained the credentials to complete wire transfers.

The IBM researchers conclude their report saying "[T]his campaign highlights the fact that organizations are only as strong as their weakest link, and in this case, it's their employees. IBM's Cyber Security Intelligence Index indicated 95 percent of all attacks involved some type of human error. These attackers rely on that factor so someone will open a suspicious attachment or link and they can successfully steal millions." Based upon our experience, we couldn't agree more. That's why training your employees is a key risk management tool for your organization.

– Linn Foster Freedman

DATA BREACH

Wyoming amends data breach notification law

Continuing to add to the confusion surrounding provisions in 47 different state breach notification laws, Wyoming amended two laws last month which expand the definition of personal information requiring notification in the event of a breach starting in July of 2015.

Specifically, the definition of personal information was amended to include an individual's first name or first initial or last name in combination with any **one or more** of the following data elements, when the data elements are not redacted: (1) Social Security number, (2) driver's license number, (3) account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person, (4) tribal identification card, (5) federal or state government issued identification card, (6) shared (login) secrets or security tokens known to be used for data based authentication purposes, (7) a username or email address when combined with a password or security question and answer that would permit access to an online account, (8) a birth or marriage certificate, (9) medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, (10) health insurance information, meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person's application and claim's history, (11) unique biometric data, or (12) an individual taxpayer identification number.

This broadened definition will certainly capture additional incidents involving the loss of personal information requiring notification in Wyoming. As we stated about the amendment to the Montana law [insert link here], we anticipate that additional state laws will be passed expanding the definition of personal information consistent with these two laws, so it is important to stay abreast of the amendments nationally in the event a company suffers a data breach. We will continue to report on changes to state breach notification laws as they are amended.

– Linn Foster Freedman

SOCIAL MEDIA

New York court permits plaintiff to serve divorce summons through Facebook message

The Manhattan Supreme Court recently permitted the plaintiff in divorce proceedings to serve the divorce summons to her husband through a private Facebook message. Justice Matthew Cooper acknowledged that the plaintiff's request for sole, and NOT supplemental, service through a social media message was a "radical departure" from the judicial standard. In Justice Cooper's opinion, he wrote, "In this age of technological enlightenment, what is for the moment unorthodox and unusual stands a good chance of sooner or later being accepted and standard, or even outdated and passé." *See Baidoo v. Blood-Dzraku*. This decision is considered out of the box because while other judges have allowed service through Facebook messaging, it has typically only been allowed when such service is IN ADDITION to other more

standard methods of service. Justice Cooper said that the because the plaintiff had submitted an affidavit vouching that the Facebook account was that of the defendant, her husband, and that she provided exhibits showing prior message exchanges that the couple had on Facebook, this new form of service was perfectly acceptable. You never know what you'll find in your Facebook inbox.

– Kathryn M. Sylvia

DATA PRIVACY

What are you wearing? Data from wearables could soon be introduced as evidence

Whether you are tracking your steps, your calories or the amount of water you drink, the data collected by your wearable devices could open up a whole new can of worms in court. In a San Jose, California personal injury case, the plaintiff's attorney is attempting to get all that wearable device data into evidence at trial later this year. The case centers around the claim that the plaintiff's activity was significantly reduced due to an accident. Plaintiff's attorney hopes to introduce this data to support that claim. However, how reliable is that data? While many experts say that data from wearable devices will soon enter the courtroom, there are several concerns. The first concern: reliability. Some devices may log physical activity if say you are sitting on your couch binge watching your DVR waving your arms around. Or maybe you forgot to wear the device all together one day. Therefore, the evidence from wearables likely won't be able to stand on its own without expert testimony or other corroborative evidence. The second concern: privacy and ownership of the data. While the federal Health Insurance Portability and Accountability Act (HIPAA) does not regulate the data collected by these devices, if the devices are linked to more specific health care information, it could be a very slippery slope. And the last concern: opening clients to cross-examination. If plaintiffs' attorneys present the data to confirm their claims, it does open up the plaintiff to cross-examination regarding the same. It may also give defendants' attorneys a reason to seek their own data. However, this data could serve a valuable purpose in many types of litigation. Just remember, beware of what you are wearing around your wrist. It could paint a picture that doesn't look so good.

– Kathryn M. Sylvia

MERGERS + ACQUISITIONS

Informatica snagged by private equity group and pension investment board for $5.3 billion

Proving that big data and digital companies continue to intrigue big investors, big data analytics company Informatica has been purchased by private equity group Permira and the Canada Pension Plan Investment Board for $5.3 billion. It is reported as being the largest leveraged buyout thus far in 2015. Informatica, which provides analytics, cloud computing and information security services to its brand name clients, brought in revenue of $1 billion in 2014.

– Linn Foster Freedman

Playtech Enters Foreign Exchange Market

Online gaming software company Playtech Ltd. has announced that it is purchasing TradeFX for close to $499 million, representing just over 91% of TradeFX's worth. Playtech's acquisition of TradeFX, which operates the site markets.com, will launch it into the foreign exchange world as TradeFX offers a trading platform for foreign currencies, binary options and deliverables. Playtech stated that with the acquisition of TradeFX, Playtech will be able to offer TradeFX's services to its existing online gaming clients.

– Linn Foster Freedman

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
