June 4, 2015

SOCIAL MEDIA

Oregon Social Media Law Signed By Governor

Yesterday, Oregon Governor Kate Brown signed into law a new social media law in Oregon, the first in the nation, that limits employers from requiring employees to have social media accounts for employment, and to require workers to advertise on their personal social media accounts.

The facts behind the bill are interesting. The bill's primary sponsor's wife had a friend, a Navy veteran, who returned from service and applied for a job at a sporting goods chain. He applied for the job online, and the company called him and advised that he had left his Facebook account blank on the application. When he advised that he did not have a Facebook account, the company allegedly told him they would not interview him unless he had one.

Oregon already has a social media law on the books that does not allow employers to require employees to divulge their social media passwords so the employer can access the social media accounts. States are following suit, and we anticipate that other states will think Oregon's new social media law is a good idea and no doubt, we will see other states implementing similar laws in the near future.

– Linn Foster Freedman

SCOTUS Rules Facebook Posts Not Threatening Without Intent

The Supreme Court of the United States of America (SCOTUS) ruled on June 1, 2015, that violent Facebook posts of a husband about killing his wife with a mortar launcher and blowing up FBI agents cannot be considered threatening if the author alleges he did not intend for it to be perceived that way. The decision had the effect of vacating the conviction of the husband on five counts of making threatening communications. He had been sentenced to 44 months in prison.

The crux of the decision was that the trial court had instructed the jury that the standard for determining whether the statements were threatening was a "reasonable person" standard and how a reasonable observer would take the message, rather than whether or not the speaker intended for the posts to be threatening. SCOTUS held that some sense of intent and wrongdoing was required to establish criminal conduct. The reasonable person standard would be appropriate for civil liability, but not for criminal liability and a criminal conviction for making threatening communications.

Justice Alito stated in his dissenting opinion that he felt the majority opinion would "cause confusion and serious problems" because there was no explanation by the majority as to what type of intent is

necessary to elevate the posts to threatening enough to become criminal. The husband argued all along that he did not mean for the posts to be threatening.

The decision attempts to balance allowing what might be perceived as offensive speech protected by the First Amendment and speech that is intended to have an impact on the receiver. However, as pointed out by the dissenters, SCOTUS failed to provide a clear standard as to what intent is necessary for social media speech to rise to a criminal offense. The law in this area will continue to develop as social media issues wind their way through the court system.

– Linn Foster Freedman

ENFORCEMENT + LITIGATION

Judge Tosses TCPA Action, AOL Not In Violation

On May 29, 2015, U.S. District Court Judge Ronald M. Whyte tossed out a Telephone Consumer Protection Act (TCPA) claim against AOL, Inc. (AOL) because he found that the TCPA regulations did not apply to the messages received by the plaintiff.

Plaintiff, Nicholas Derby, filed his complaint back in February 2014, alleging that an unnamed individual accidently sent him three text messages through AOL instant messenger, which he believed constituted an automated telephone dialing system message, which is prohibited by the TCPA without first obtaining consent. Derby also claimed that AOL violated the TCPA because the company sent him an automated reply to a text message it received from Derby requesting that the user who was erroneously texting him be blocked from messaging Derby. Derby was seeking an injunction and $500 per violation. However, Judge Whyte said in his opinion, “As to the initial three texts, there was sufficient human intervention to remove them from the scope of TCPA liability. Second, the TCPA does not impose liability for confirmation texts like those alleged in the complaint.” This is a success not only for AOL but for other companies whose services involve human interaction and automated text message replies to consumer text messages.

– Kathryn M. Sylvia

Target and MasterCard Settlement Rejected

We previously reported on the efforts of Target to settle claims made by MasterCard and its issuers as a result of the infamous Target data breach. In order for the settlement of $19 million to reimburse banks and credit unions for costs associated with re-issuance of credit and debit cards to become effective, 90% of the affected banks and credit unions had to agree to the settlement by May 20th. The threshold was not reached by the deadline, and therefore, the settlement will not become effective and Target will have to continue to defend the lawsuits filed by the card issuers.

– Linn Foster Freedman

Seizure of Memory Cards From Digital Cameras Allowed Under Plain View Doctrine

Courts today are faced with applying traditional Fourth Amendment search and seizure doctrines to

twenty-first century digital technology. In one such case, the Massachusetts Appellate Court upheld a lower court's holding in *Commonwealth v. Tarjick*, 87 Mass. App. Ct. 374 (App. Ct. 2015) denying a motion to suppress memory cards that were seized during a warrant search but were not listed on the warrant. Police were executing a search warrant for nude images of the defendant's minor stepdaughter on a video camera, cellphone, and computer, when they encountered the digital cameras at issue.

The decision held that police were justified in seizing three memory cards from digital cameras under the plain view doctrine. The plain view doctrine applies:

> (1) where the police are lawfully in a position to view the object
>
> (2) where the police have a lawful right of access to the object; and
>
> (3) in cases concerning (a) contraband, weapons, or other items illegally possessed, where the incriminating character of the object is immediately apparent; or (b) other types of evidence ('mere evidence'), where the particular evidence is plausibly related to criminal activity of which the police are already aware.

The Court held that the memory cards were "plausibly related to criminal activity" because the police officers were aware that data could be transferred from one device to another through the memory cards, and thus, the memory cards could have contained the images detailed in the search warrant. It noted that "[c]onsidering the constantly evolving nature of technology, we do not reach the issue whether the police in this case could have included in their application for the original warrant, any memory cards capable of storing digital images or recordings."

– Kathleen E. Dion

CYBERSECURITY

Assessing Cybersecurity Risks and Protecting Consumer Data Before Filing For an IPO In The Age of The Internet of Things

In May of this year, Fitbit Inc. (Fitbit) filed for an Initial Public Offering (IPO) for upwards of $100 million. With more and more consumers using wearable devices, privacy concerns have skyrocketed. However, since 2011, the U.S. Securities and Exchange Commission (SEC) has required publicly traded companies to disclose potential risks and threats to their security when filing their S-1 IPO forms, most likely due to the increased presence of the "Internet of Things" and our connected devices. With our cars talking to our iWatches and our refrigerators sending messages to our grocery store mobile apps when we run out of milk, it is becoming increasingly important for companies to analyze cybersecurity risks and ensure that systems are in place to protect consumer data. And investors want to know that data privacy and security is on the company's radar.

For example, in filing its S-1 form with the SEC, Fitbit disclosed, "If our security measures, some of which are managed by third parties, are breached or fail, unauthorized persons may be able to obtain access to sensitive user data. If we or our third-party service providers, business partners, or third-party apps with which our users choose to share their Fitbit data were to experience a breach of systems compromising our users' sensitive data, our brand and reputation could be adversely affected, use of our products and services could decrease, and we could be exposed to a risk of loss, litigation, and regulatory proceedings." This could be a big concern for Fitbit investors. If investors stand a chance of losing profits because of a company's lax data privacy and security practices, even if those practices are that of a third-party service provider, the investment in that company may not seem so tantalizing. Companies surely know that a data breach not only affects its customers, it can also affect the company's pockets as well. Bad press will certainly drive customers away.

Before companies enter the public markets, they are not only required by the SEC to assess and disclose their cybersecurity risks, but investors will demand that they have appropriate privacy and security policies and procedures in place to protect consumer data. Investors will surely consider a company's cybersecurity risks along with the IPO valuation.

– Kathryn M. Sylvia

DATA BREACH

Sally Beauty Reports 2nd Data Breach

Late last week, Sally Beauty Holdings, Inc. (Sally) confirmed that it has suffered a second data breach in the last year. On March 14, 2014, KrebsOnSecurity reported that credit cards stolen from Sally had gone up for sale on an Internet site. Reportedly a data breach occurred when intruders gained access through a Citrix remote access portal for employees to log into the Sally system while working remotely. Sally later confirmed that approximately 25,000 records had been accessed and removed from its system by the hackers, impacting all of its stores.

Sally confirmed on May 28th that hackers have accessed its customers' debit and credit card information through its point of sale systems. The intruders were able to install malware, which was active from March 6th to April 17th. Sally stated it has removed the malware and is offering credit monitoring for its customers.

– Linn Foster Freedman

DRONE PRIVACY

DOJ Releases Guidelines On Drone Operation By Federal Law Enforcement

Last week, the U.S. Department of Justice (DOJ) published guidelines for the use of unmanned aerial vehicles (UAVs) or, as more commonly called, drones, by federal law enforcement. Currently, the FBI is the only agency using drones, but in light of the recent rise in drone use for kidnapping investigations, search and rescue operations, drug interdictions, and fugitive investigations, the DOJ released these guidelines to stay ahead of the game.

Here is a summary of those guidelines:

- **Respect for Civil Rights and Civil Liberties**: The guidelines state "respect for civil rights and civil liberties is a core tenet of our democracy." Therefore, federal law enforcement must use drones in accordance with the First and Fourth Amendments, and only "with properly authorized investigations and activities."
- **Protection of Privacy**: The guidelines state that the DOJ "operates under a set of rules, policies, and laws that control the collection, retention, dissemination and disposition of records that contain personally identifiable information." The guidelines explain that those same rules, policies and laws apply to the data collected through drone operation. To ensure compliance, the Senior Component Officials for Privacy in each federal law enforcement agency "must conduct annual privacy reviews of their agency's use of [drones]."
- **Accountability**: The guidelines state that "personnel [must be] appropriately trained and

supervised," and in accordance with the Federal Aviation Administration's (FAA) guidelines, all drone operators must be certified.

- **Ongoing Policy Management**: The guidelines require that all federal law enforcement agencies "report annually to the Deputy Attorney General on the use of [drones]."
- **Transparency**: Lastly, the guidelines state the DOJ seeks to enhance "transparency about agency operations, including how we operate [drones], [to] create an informed citizenry and greater confidence in the [DOJ's] decision-making." The DOJ seeks to educate the public as it continues to use drones for investigations and begins using drones in new ways to help aid investigations.

This is a substantial step in the right direction for protection of citizens' privacy rights as more and more drones start flying above our heads.

– Kathryn M. Sylvia

Mountain High Aviation Receives Approval From FAA To Fly Wildlife Monitoring Drones

On May 28, 2015, Mountain High Aviation LLC (MHA) received the okay from the Federal Aviation Administration (FAA) to fly its drones in U.S. airspace under the FAA Modernization and Reform Act. MHA is a wildlife monitoring service based in Oregon that applied for an exemption under the FAA framework to use four drones to serve companies in remote sensing, mining, mapping, precision agriculture, real estate, and energy industries. MHA said in its application to the FAA that it provides an opportunity for wildlife monitoring with aircrafts that eliminate many of the risks associated with manned aircrafts, such as reliance on flammable fuel. Of course, much like Amazon's exemption approval from the FAA, MHA cannot use drones weighing more than 55 lbs. or at heights above 400 feet, and cannot fly their drones faster than 100 mph. MHA is also prohibited from flying their drones at night or above closed-sets for TV and movies. While this is certainly a step in the right direction for MHA, the FAA will need to loosen its standards to permit more use of these unmanned drones that can certainly be beneficial in many ways; however, the standards can only be loosened after the FAA sets forth some better privacy standards for these aircrafts.

– Kathryn M. Sylvia

HEALTH INFORMATION

Teladoc Successful In Thwarting New Texas Telemedicine Rules

We previously reported on the new telemedicine regulations adopted by the Texas Medical Board (Board), which requires that patients be seen face-to-face or in person to establish a physician-patient relationship in order to provide telehealth services. The rules were to go into effect yesterday.

Teladoc Inc., a telehealth services provider, challenged the regulations and filed suit against the Board seeking a preliminary injunction to stop the regulations from going into effect under federal antitrust laws, saying it unlawfully restrained competition in the provision of health-care services.

The U.S. District Court for the Western District of Texas agreed with Teladoc and held that Teladoc had shown that it was likely to succeed on the merits of its claim that the rule violates Sherman Act Section 1, 15 U.S.C. § 1. This section makes unlawful any contract, combination or conspiracy to restrain trade. The Court found that Teladoc would be irreparably harmed if the rule went into effect and therefore, issued the injunction.

– 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 + 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.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

---