NOW + NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

March 8, 2019

What's trending on NP Privacy Partner

An actor's tweet ruled to be non-defamatory, the Third Circuit upholds injunction in favor of company monitoring ex-employees' Facebook communications and more. Here's what's trending in data privacy and cybersecurity.

Social Media

Actor's tweet ruled to be non-defamatory

The United States Court of Appeals for the Sixth Circuit has ruled that a tweet posted by Hollywood actor James Woods contained sufficient ambiguity to avoid defamation liability to a plaintiff who claimed that Woods wrongly portrayed her as giving a Nazi salute at a Donald Trump 2016 presidential rally. The court held that the inclusion of a question mark could deem the tweet to be posing a question rather than expressing a statement of fact.

Portia Boulger, who supported Democratic presidential candidate Bernie Sanders in the 2016 election season, sued Woods for defamation after the actor tweeted a photo of Boulger alongside another photo of a woman making a Nazi salute at a Trump rally. Woods' tweet implied that Boulger may have been a plant at the rally by tweeting "So-called #Trump 'Nazi' is a #BernieSanders agitator/operative?" It was later confirmed that the woman giving the salute was not Boulger, but another person. Woods deleted the tweet with an apology to Boulger. Boulger sued Woods for defamation, which an Ohio federal district court dismissed at the pleadings stage. Boulger appealed to the Sixth Circuit.

The Sixth Circuit analyzed the tweet under Ohio law's "four-prong, totality-of-the-circumstances test" to determine whether Woods published a false statement of fact, and addressed "the issue of whether questions can (or cannot) be defamatory." The four factors are: (1) the specific language used, (2) whether the statement is verifiable, (3) the general context of the statement and (4) the broader context in which the statement appeared.

Regarding the first factor, the appellate court found that some readers of the tweet likely viewed it as an insinuation that Boulger was the women in the photo giving the salute, but it seems equally plausible that the tweet was posing a question such that its content had a precise meaning. Analyzing the second factor, the court held that the tweet did not present an obvious example of a question that could be factually verified, which requires reviewing its context under the third and fourth factors. Woods is a tweeter of politically charged content with sarcasm, exaggeration and hyperbole—characteristics more likely to be seen in an opinion, rather than a statement of fact.

Woods' tweet with Boulger's photo is reasonably susceptible to both a defamatory meaning—that Woods was asserting she was the woman giving the salute, and an innocent meaning—that Woods was merely asking his readers a question. Because the tweet could reasonably be read to have an innocent meaning, it is not actionable as a matter of law.

A concurring opinion, agreeing with the result, stated that application of the four-part test is awkward in this social media context. The analysis simply requires asking whether a reasonable reader would interpret the tweet as a genuine question. Regarding Woods' tweet, the inclusion of the question mark assumes that the writer is asking a question, such that a reasonable reader would not interpret it as an implied statement of fact. –*Steven M. Richard*

Privacy Litigation & Class Action

Judge finds Washington's cyberstalking law to be unconstitutional

Washington federal judge has ruled that the state's law prohibiting cyberstalking is facially unconstitutional under the First Amendment to the United States Constitution, as made applicable to the states through the Fourteenth Amendment. In 2004, Washington enacted one of the first state statutes directly criminalizing cyberstalking. The provision challenged in the litigation provides that a "person is guilty of cyberstalking if he or she, with intent to harass, intimidate, torment, or embarrass any other person . . . makes an electronic communication to such other person or a third party . . . makes an electronic communication to such other person or a third party . . . anonymously or repeatedly whether or not conversation occurs."

The lawsuit was filed by a retired Air Force major, Richard Rynearson III, an online author and activist who regularly posts comments related to civil liberties that are critical of police abuse and expansions of executive power since the September 11 terrorist attacks. Much of his online commentary relates to a detention provision in the National Defense Authorization Act (NDAA), and he became interested in public and civic organizations in the Seattle area that memorialize or seek to present the lessons of the Japanese-American internment during World War II. Rynerason regularly posts comments on Facebook pages critical of civic leaders and organizations that fail to condemn the NDAA or detention issues. He posted numerous criticisms on his neighbor's Facebook page and later created a group using his neighbor's name. Rynearson's activities made him the subject of police reports and civil protection orders.

Rynearson filed suit contending that the Washington statute criminalizes plainly protected speech under the First Amendment. The Washington Federal District Court found that the statute's breadth included protected speech and criminalizes a large range of non-obscene, non-threatening speech, based only on purported bad intent and repetition or anonymity. Particularly, the United States Supreme Court has consistently classified emotionally distressing or outrageous speech as protected, especially where that speech touches on matters of political, religious or public concern. As the court has held, this is because "in public debate our own citizens must tolerate insulting, or even outrageous, speech in order to provide 'adequate breathing space' to the freedoms protected by the First Amendment." The Washington cyberstalking law's prohibitions against speech that is intended to "harass, intimidate, torment, or embarrass" were too vague to withstand constitutional scrutiny. – *Steven M. Richard*

Third Circuit upholds injunction in favor of company monitoring ex-employees' Facebook communications

The United States Court of Appeals for the Third Circuit has upheld a preliminary injunction that Scherer Design Group, LLC (SDG), an engineering firm, obtained against four former employees, stopping them from contacting SDG's clients and destroying information taken from SDG. The defendants asserted that SDG surreptitiously monitored one of the former employees' Facebook activity after he left SDG and claimed that the company's "unclean hands" barred it from obtaining equitable relief. The Third Circuit ruled that the federal trial court acted within its discretion in declining to apply the unclean hands doctrine against defendant's former employer. Scherer Design Group, LLC v. Ahead Engineering LLC, et al., No. 18-2835 (3rd Cir. Feb. 25, 2019).

One of the defendants, Chad Schwartz, left SDG after a dispute over whether he was promised an equity partnership in the engineering firm. Before resigning, Schwartz declined to sign a noncompete agreement. After resigning, Schwartz started two competing engineering firms and recruited SDG employees to join his new firms. Three SDG employees discussed Schwartz's new venture with him using, in part, Facebook, and transmitted SDG documents and information to Schwartz's firms. The three employees eventually resigned from SDG to work with Schwartz.

After the mass loss of employees and a key customer account, SDG's network administrator examined the former employees' SDG computers. One of those former employees, Daniel Hernandez testified that while working at SDG, he accessed his Facebook account from his SDG laptop and "would log off sometimes and leave it open sometimes," but that on the day he resigned from SDG he closed out of Facebook by clearing the history on the internet browsers on his SDG laptop. SDG's network administrator (1) reviewed Hernandez's browser history using software that allowed him to access deleted activity, (2) asserted that he was able to access Hernandez's Facebook account without a password because Hernandez had not cleared it from the laptop and (3) installed software that allowed him to monitor Hernandez's Facebook activity without detection. For several weeks after the exit of the employees, the administrator accessed Hernandez's Facebook account "very often" from Hernandez's laptop and uncovered messages that revealed the defendants' plans and actions taken to secure SDG's client information and other intellectual property.

In litigation, the parties disputed how SDG gained access to Hernandez's Facebook account, and the defendant employees opposed any injunctive relief against them by contending that their former employer's secret monitoring left it with "unclean hands," thus precluding its request for injunctive relief. The "unclean hands" doctrine is not an automatic or absolute bar to injunctive relief, but rather one factor to apply in the equitable analysis. A party seeking to invoke the doctrine must show: (1) the party seeking equitable relief committed an unconscionable act; and (2) the act is related to the claim upon which equitable relief is sought.

In affirming an injunction in favor of SDG, the Third Circuit cited three grounds. First, SDG did not dirty its hands to "acquire the rights" that it asserts in the complaint. SDG did not monitor Hernandez's Facebook account so it could obtain a right it did not otherwise have. Defendants owed a duty of loyalty to SDG well before the Facebook monitoring occurred. Second, while SDG obtained proof of its duty of loyalty claim from its monitoring and benefitted from its activity, it had a right to defendants' loyalty and could prove their breach without relying on the surreptitiously obtained Facebook messages, as SDG was able to corroborate all of the messages among the defendants. SDG's monitoring of the Facebook messages was not related to whether the defendants earlier stole SDG's property. Third, SDG's alleged privacy violation and defendants' alleged breach of duty of loyalty are causes of action subject to distinct bodies of law and with

separate remedies. In sum, because relatedness is a critical element of the unclean hands doctrine and SDG's allegedly unclean hands are not directly related to the defendants' breaches of their duty of loyalty, the Third Circuit ruled that the trial court did not abuse its discretion in declining to apply the unclean hands doctrine to prevent SDG from obtaining injunctive relief.

A dissenting opinion disagreed with the majority's analysis, citing to the requirements of New Jersey privacy law. The dissent concluded that SDG's activities were tortious based upon New Jersey case law regarding employer monitoring of personal e-mails from work accounts and the standards for invasion of privacy claims.

The ruling presents a common occurrence in business dealings, especially where there are no noncompete or nonsolicitation agreements in place applying to employee departures. Before engaging in similar monitoring as SDG's actions, a company should carefully consult with counsel to evaluate the extent to which company policies and controlling jurisdictional law will permit the review and monitoring of social media and private e-mail accounts, particularly as to former employees. – *Steven M. Richard*

Financial Institutions

FTC seeks comments on proposed amendments to Safeguards and Privacy Rules to GLBA

On March 5, the Federal Trade Commission announced that it will soon publish notices in the Federal Register seeking comments on proposed changes to the Safeguards Rule and the Privacy Rule under the Gramm-Leach-Bliley Act. The proposed changes seek to align the rules with changes implemented by Congress through the Dodd-Frank Act in 2010 and the FAST Act in 2015.

Enacted in 2003, the Safeguards Rule requires a financial institution to develop, implement and maintain a comprehensive information security program. Enacted three years earlier in 2000, the Privacy Rule requires a financial institution to inform customers about its information-sharing practices and to afford opt-out rights to prevent information sharing with certain third parties. The FTC voted 3–2 to publish the proposed amendments to the Safeguards Rule, while the proposals relating to the Privacy Rule passed by a unanimous 5–0 vote.

The proposed changes to the Safeguards Rule seek to add more detailed requirements for the contents of a comprehensive information security program. For example, financial institutions would be required to encrypt all customer data, implement access controls to prevent unauthorized users from accessing customer information and use multifactor authentication access to customer data.

The enactment of the Dodd-Frank Act narrowed the scope of the Privacy Rule, transferring the majority of the FTC's rulemaking authority to the Consumer Financial Protection Bureau, leaving the FTC with rulemaking authority over certain motor vehicle dealers. The FTC has proposed to remove from the Privacy Rule examples of financial institutions that do not apply to motor vehicle dealers.

Copies of the notices and proposed changes may be viewed on the FTC's website at www.ftc.gov. Comments must be received within sixty days after publication in the Federal Register and will be posted on Regulations.gov. We will monitor the comments and the course of the proposed regulatory amendments. – *Steven M. Richard*

Cybersecurity

New federal data privacy bill encounters state roadblocks

In the wake of the seemingly endless stream of data privacy scandals that surfaced over the past year, lawmakers have renewed the push for the nation's first comprehensive, bipartisan data privacy law. However, at the start of the first hearings on the matter in the current Congress, legislators have encountered a major roadblock, namely, conflicting state regulations that attempt to cover consumer privacy issues.

State legislatures were spurred into action in 2018 as the number of data privacy breaches mounted. In June 2018, California became the first state to pass a consumer privacy law when then-Governor Jerry Brown signed the California Consumer Privacy Act (the "CCPA") into law. The CCPA, the requirements from which do not go into effect until January 1, 2020, poses hurdles for business both inside and outside of California. The CCPA applies to for-profit entities that collect and process the "personal information" of California residents. While an entity must do business in California in order to be subject to the CCPA, physical presence in California is not a requirement. The definition of "personal information" is much broader than typically seen in U.S. privacy laws, and includes "information that identifies, relates to, describes[] [or] is capable of being associated with . . .a particular consumer or household.[1]" Other states [2] have expanded definitions relating to personal identifying information in privacy-related laws.

With Congress now addressing the first federal data privacy law in U.S. history, many on both sides of the aisle fear that a patchwork of state regulations may, at best, lead to confusion amongst businesses having to deal with conflicting regulations, and, at worst, may preclude smaller businesses from being able to comply. Preemption is a potential solution to this issue, and legislators have certainly not ruled out the possibility of preemption if the federal bill is able to adequately protect U.S. consumers. The fear amongst Democrats, however, is that Republican lawmakers seek to pass a federal privacy bill simply as a means to preempt the CCPA, a bill which many Republican lawmakers and industry group members oppose. Whether legislators will be able to come together for a bipartisan agreement sufficient to justify preemption remains to be seen. – *Wesley Gangi*

For more information, please contact:

- Steven M. Richard at **srichard@nixonpeabody.com** or 401-454-1020
- Wesley Gangi at **wgangi@nixonpeabody.com** or 312-977-4478

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team