masuda funai

News & Types: Employment, Labor & Benefits Update

Workplace Privacy in California

8/28/2018

Practices: Employment, Labor & Benefits

Author: Asa Markel
Co-Author: Miho Lee (Law Clerk)

EXECUTIVE SUMMARY

California recently passed one of the strictest data privacy laws in the country, the California Consumer Privacy Act of 2018, which will go into effect on January 1, 2020. While the new law only applies to consumers and businesses which collect and sell consumer information for commercial purposes, all employers maintain confidential personnel information, and accordingly have the duty to protect such information from various kinds of breaches. Such breaches include workplace invasion of privacy, whether the intrusion is by the employer or a fellow employee. While employees are generally granted only a reasonable expectation of privacy at the semiprivate workplace, employers must still ensure that they refrain from unreasonable surveillance methods, as well as ensure the protection of employees' rights under California's constitution.

The Northern District of California currently has at least one lawsuit involving a British data mining firm co-founded by Stephen Bannon, the campaign manager and the former White House strategist for Donald Trump. Bannon's firm, Cambridge Analytica, was responsible for accessing the data of millions of people, and allegedly used such data during the 2016 presidential election. The California Consumer Privacy Act of 2018 (the "Act") was recently passed against the backdrop of such political and social turmoil. It also emerged immediately following the coming into force of the General Data Protection Regulation ("GDPR") of the European Union.

California currently already has several laws regulating certain privacy rights. For example, the Information Practices Act of 1977 protects individuals from governmental agencies' violations of data privacy rights. In addition, the Online Privacy Protection Act of 2005 regulates commercial online service operators' handling of the personal data of individual consumers including minors residing in California, and California's Civil Code imposes safeguards on the handling of consumers' personal data by businesses they deal with. However, although there are many laws enacted to protect individual privacy from the government handling of personal data, or from businesses which utilize personal information for commercial purposes, protection of privacy at the workplace is still an area governed by common law.

There are four basic concepts relevant to the common law torts of invasion of privacy. Like most American states, California recognizes all four torts: intrusion upon seclusion; public disclosure of private facts; false light; and appropriation of name or likeness. When someone has committed one of these torts, the public often

hears that there has been an “invasion of privacy.” However, the level of workplace privacy granted to employees depends on the case-by-case circumstances.

One of the aforementioned common law torts, intrusion upon seclusion, or the “right to be left alone,” protects employees against an employer’s wrongful intrusions on employees’ protected privacy interests. However, the “intrusion” must be highly offensive to a reasonable person, and the employee’s reasonable expectation of privacy must be weighed against the employer’s business justification for the intrusion. Since it is a normal practice for employers to monitor their employees’ computer use, one of the chief concerns for employees may be their employers’ surveillance or control of employee activities through the use of company electronic devices.

In *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272 (2009), the Supreme Court of California found that the employer’s intrusion was not so highly offensive as to constitute a privacy violation, especially where the employer had good reasons for the surveillance. In *Hernandez*, the employer installed video surveillance equipment in certain employees’ offices for the purpose of catching a culprit who evidently accessed pornographic websites during late evenings and sometimes into the early morning hours when the said employees were not present. Since the employer ran a residential treatment center housing many emotionally and physically abused children, some of whom were previously exposed to pornography, the security measure was imperative in order to preserve the welfare of those children.

In *Hernandez*, the plaintiffs were two female employees who shared an office which could be locked if they wished. In fact, one of the employees often locked the door just before leaving work in order to change out of her work clothes into gym clothes. However, the *Hernandez* court found that the employer’s surveillance activities were limited in scope and duration, and never actually caught either of the plaintiffs on camera. The monitoring took place only once a week for a three-week period, and only after the said employees’ shifts had ended, which corroborated the employer’s assertion that the surveillance equipment was installed for a purpose other than invading the employees’ privacy. In addition, the underlying activities which the employer intended to uncover clearly violated their written “E-Mail, Voicemail and Computer Systems Policy” which expressly prohibited the use of the employer’s electronic communications system in an inappropriate manner which, considering the nature of the business, could potentially subject the company to legal exposure. After considering all of the above circumstances, the Court ruled that the employer’s use of the surveillance systems was “narrowly tailored in place, time, and scope” as well as “prompted by legitimate business concerns.” However, *Hernandez* also demonstrates that if the employer had not been careful to address only legitimate business concerns, an invasion of its employees’ privacy could expose the employer to civil damages.

Action Steps: As shown in *Hernandez*, even though California’s data protection legislation may not directly apply, employees still have protectable privacy rights as a matter of long-standing common law. Every employer in California should ensure that it has legally compliant, written policies in place which detail the rules for the usage of company-owned equipment as well as employee-owned electronic devices at the workplace, and spell out what expectations employees should have concerning privacy in the workplace.