Welcome

Across the economy, businesses are using digital technology to pivot into innovative service lines, accelerate growth and transform their businesses altogether. These businesses' digital strategies and data assets play important roles in their success. Since the advent of the COVID-19 pandemic in the United States in March 2020, companies that had the technology to enable their employees to work from home have shut down their offices, in some cases forever. In this issue, we are highlighting Jerel Pacis Agatep and how his privacy practice, and background in labor and employment law, intersects with digital transformation and data economy.

Spotlight

Jerel Pacis Agatep addresses the top six privacy and security issues for remote workforce monitoring

In recent years, employer liability for invasion of privacy has increasingly become one of the top legal issues for in-house legal teams. Litigation claims related to invasion of privacy torts include common law claims such as (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) false light and (4) misappropriation. Several federal (e.g., Title VII, ADA, FMLA, OSHA and FSLA) and state laws also have requirements as to record retention and reasonable destruction and disposal (e.g., FACTA and FCRA) of personal information. Outside of general employee privacy considerations, we look at some specific scenarios below that have become more critical, especially as employers are responding to the COVID-19 pandemic.

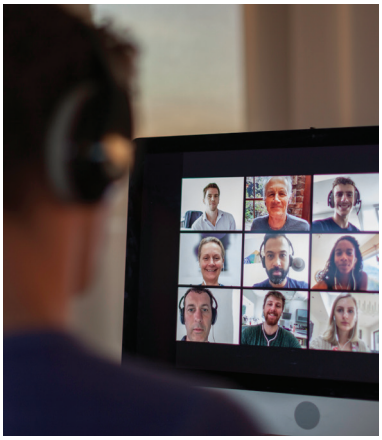
The Electronic Communications Privacy Act (ECPA) is the principal federal law that addresses an employer's right to access certain types of communications made in the workplace. The ECPA prohibits the interception and monitoring of "electronic communications." The ECPA consists of two main component laws: The Wiretap Act and the Stored Communications Act (SCA). The Wiretap Act applies only to electronic communications in transit, while the SCA applies to electronically stored information.

In addition to the ECPA, many states have enacted laws pertaining to the interception of electronic communications. The majority of these states' laws (38 out of 50 and D.C.) – like the federal Wiretap Act – require the consent of only one party to the conversation. Twelve states' laws – California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Missouri, Nevada, New Hampshire, Pennsylvania and Washington – require two-party consent, with some distinction as to whether communication is electronic or in person.

Spotlight (cont'd.)

Lastly, although the U.S. Constitution does not have an explicit provision regarding an individual's right to privacy, the constitutions of at least 10 states (Alaska, Arizona, California, Florida, Hawaii, Louisiana, Montana, New Hampshire, South Carolina and Washington) have express provisions relating to their constituents' right to privacy.

Below, we discuss the privacy and security pitfalls that employers have become aware of as the workplace continually expands toward what employees used to consider private space – their homes.



1. Email and Text Monitoring

Monitoring employees' email and text communications presents numerous problems. First, even though the different federal and state laws provide employer exemptions (e.g., consent, business exemption, service provider exemption) allowing them to monitor their employees, employers must still be cognizant of employees' reasonable expectation of privacy, especially in states where such right to privacy is afforded by the state's constitution. "Expectation of privacy" is on a sliding scale and can be interpreted on a caseby-case basis, so employers should err on the side of caution. For example, an employee may have a greater expectation of privacy when using personal email versus work email. Second, employers may be liable for breach of data security in the event that personal, sensitive and trade secret information is inadvertently disclosed or shared by an employee's misuse of the company's electronic communications platforms.

2. Oral Communication (Telephone and Voicemail)

Employers may monitor oral communication under the exemptions provided by the Wiretap Act. For example, the business use exception allows employers that have a telemarketing business to monitor employee telephone conversations "in the ordinary course of business," such as for quality control. However, employers should keep in mind that personal conversations of employees should not be monitored.

3. Video Monitoring and Surveillance

Almost all states have enacted their own laws relating to surveillance. The vast majority of state laws prohibit filming in areas where there is a "reasonable expectation of privacy." The definition of reasonable expectation of privacy differs from state to state and could also change case by case. However, generally, public places where there is a reasonable expectation of privacy include restrooms, locker rooms, changing rooms and bedrooms.

4. GPS and Cellphone Location Monitoring

Currently, the U.S. Constitution does not have an explicit provision regarding an individual's right to privacy besides the Fourth Amendment right against illegal searches and seizures, which generally does not apply to private employers. (See United States v. Jones, 565 U.S. 400 (2012).) However, several states have enacted laws pertaining to tracking an individual. For example, California can track a vehicle when the "registered owner, lessor, or lessee of a vehicle has consented to the use of the [GPS]," which presumably means that the location of a company-provided vehicle could be tracked without the employee's consent.

5. Social Media Monitoring

As stated above, under the federal SCA, employers are also prohibited from accessing private communications stored away from the workplace, including an employee's social media accounts (e.g., Facebook, Instagram, Twitter). Additionally, at least half of the states have enacted laws prohibiting employers from asking

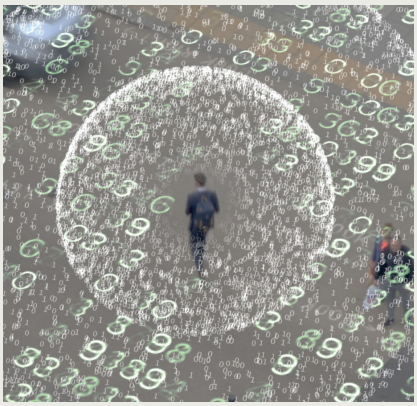
Of Recent Note

Blog Posts

New Taxes on the Digital Economy: A Closer Look at the New York Data Tax Proposal

Virginia Becomes the Second State with a Comprehensive Privacy Law

New EDPB Draft Guidance Provides Practical Scenarios for Data Breach Notification Analysis Under the GDPR



Virginia Poised to Enact the Consumer Data Protection Act, the Nation's Second Comprehensive Consumer Privacy Law

California AG Becerra Tweets Endorsement for a Universal Opt-Out Tool

Podcasts

Let it Flow: Breaking Down Information Blocking

applicants and employees for their social media login information, to access their social media in the employer's presence, to change their privacy settings to make the page accessible to the employer, or to add anyone as a "friend" or contact on a social media page. However, generally, these state laws do not prevent employers from implementing social media policies regarding use of those sites in the workplace, accessing the employee's social media related to allegations of employee misconduct or accessing information that is in the public domain.

6. Keystroke and Productivity Monitoring

Employers are generally allowed to monitor employees' activity on a company-provided device (e.g., computer or phone) or network (e.g., company VPN). This may include keystroke logging, taking screenshots, accessing the employee's hard drive and monitoring Internet usage. However, while employers may take screenshots, access employees' work hard drives and monitor Internet usage (such as social media use during work hours) to ensure employees are productive, employers must still balance their legitimate business reason with the employees' reasonable expectation of privacy (for personal discussions on social media that may be covered under Section 7 of the NLRA.)

Takeaways

In general, employers have great power when it comes to monitoring their employees. However, as Spiderman's Uncle Ben once said, "With great power comes great responsibility." Employers must not abuse this power and must be responsible when they decide to implement any of the above workplace monitoring. To avoid or mitigate any issues of employee morale, company reputation, technical logistics and legality, companies may want to consider the following best practices: (1) Review your definition of "expectation of privacy" in the workplace, (2) notify your employees regarding the types and purposes of workplace monitoring, (3) obtain voluntary consent when possible, and (4) have in place reasonable protocols and safeguards to secure employee information.

Emerging Issues

Four Ethical Considerations For Using Employee Monitoring Software On Remote Workers, *Associations Now*, March 12, 2021

The use of employee monitoring software on remote employees might seem like a smart way to handle a difficult situation, but it could raise significant ethical issues – especially if a user's work computer is also their personal one.

Remote Controlled Workers, *The American Prospect*, Feb. 24, 2021

The pandemic has allowed companies to expand an old practice of spying on workers. That's a problem for their privacy and their power.

Privacy faces risks in tech-infused post-Covid workplace, *The Economic Times*, Feb. 21, 2021

With tech-infused gadgetry to improve workplaces, employees may face screenings even as they enter a building lobby, and monitoring in elevators, hallways and throughout the workplace. The monitoring may blur the line between people's workplace and personal lives.

How employers use technology to surveil employees, *Brookings Institution*, Jan. 5, 2021

Lisa Rene worked at an Indianapolis store operated by G.F. Fishers. Without informing company employees, the firm installed keylogger software on the store's computers, which recorded characters typed on the business machines and periodically emailed that information to supervisors. When Lisa learned what had happened, she confronted her fellow employees and was fired for poor performance.

Have Your Privacy Policies Kept Up with Your Digital Transformation?, *Harvard Business Review*, June 29, 2020

For every business that shifts operations online, there are potential privacy pitfalls that will prove very damaging if mismanaged. As new regulations are set to go into force in the United States, the stakes for getting this pivot right are higher than ever before.

How to Monitor Employees While Respecting Data Privacy, *CPO Magazine*, June 5, 2020

The solutions used to monitor employees can collect a vast range of potential data including file access history, internet use, keystrokes, and email traffic. To ensure compliance with data privacy regulations, the implementation of these technologies must be properly assessed against the potential privacy impacts they can have for employees.

Nando's restaurant, Naperville lawyers reach nearly $1.8 million settlement for restaurant employees over fingerprint data lawsuit, *Chicago Tribune*, Nov. 18, 2020

More than 1,400 current and former employees of Nando's Illinois stores will receive a combined $1.787 million after a federal judge approved a settlement agreement between the South Africa-based restaurant chain and the Naperville attorneys representing the employees in a case over fingerprint data.

Businesses Nationwide Face New Privacy Rules After California Vote, *The Society for Human Resource Management*, Nov. 5, 2020

Californians just passed a ballot measure that will soon expand the nation's most stringent data privacy law – and it will have an impact on employers across the country.

H&M has been fined $41 million for violating its workers' privacy, *Business Insider*, Oct. 5, 2020

The company's service center in Germany recorded private information about "several hundred employees," including recording extensive information about family issues, religious beliefs and illnesses.