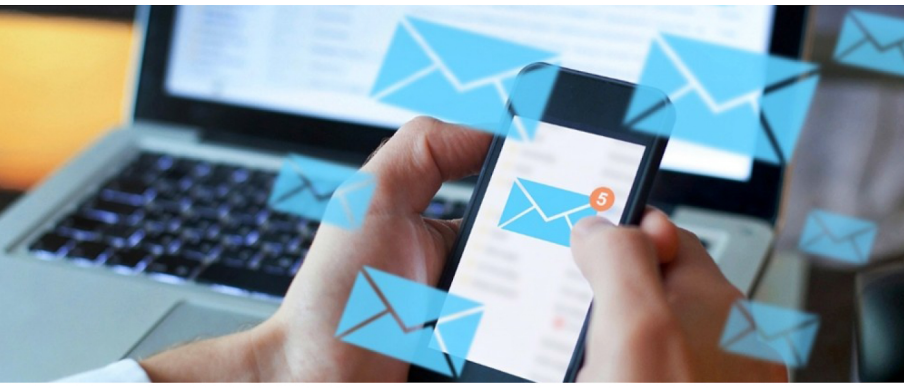
NL | LEGAL NEWS



Employers Must Think Twice Before Accessing Employee Personal Emails, Texts and Social Media Accounts

EMPLOYERS OFTEN ASSUME that company-owned devices give them broad authority to monitor employee activity. However, the Federal Stored Communications Act (SCA) places clear limits on accessing personal emails, texts, and social media accounts—even when those accounts are accessible on company-issued devices. Missteps in this area can lead to civil liability, exclusion of evidence in litigation, and potential criminal penalties.

What the SCA Protects

The SCA safeguards electronic communications stored by third-party providers, including personal email accounts, cloud-based files, and text messages retained by carriers. Importantly, the law focuses on where the data is stored, not the device used to access it. This means that even if an employee logs into a personal account on a company-issued device, the employer does not gain the right to access that account.

While employers may monitor communications sent through company systems, such as work email or internal networks,the SCA prohibits intentional, unauthorized access to employees' personal accounts, regardless of how easily accessible those accounts may be. As a result, even if a personal account is left open or login credentials are saved on a work device, accessing that information without permission may still violate federal law.

Common Risk Scenarios for Employers

Problems frequently arise during employee departures. When an employee resigns or is terminated, employers often recover devices that may still contain open applications, saved passwords, or bookmarked personal accounts. In cases where litigation is anticipated, employers may be tempted to review those accounts for useful information. However, the SCA makes clear that ease of access does not equal legal authorization. The law protects the data stored on third-party servers, not just the physical device used to access it. In other words, the employer may own the laptop, but not the employee's personal inbox.

What the Courts Say

Several key court decisions highlight the risk of overstepping the SCA boundaries and demonstrate that courts consistently interpret the SCA in favor of protecting employee privacy.

- *Pure Power Boot Camp v. Warrior Fitness Boot Camp (2010)*: A business owner accessed a former employee's personal email accounts using auto-saved credentials on a company computer. The court found that his actions violated the SCA and barred the use of those emails in litigation.
- *Levin v. Impact Office (2017)*: A former employee claimed that her employer accessed her personal emails multiple times after her departure. The court rejected the employer's argument that opened emails were not protected.
- *Benz v. PHB Realty Company (2022)*: An employee alleged her employer accessed her personal email and social media accounts without consent and then used that information to justify termination. The court allowed her SCA claim to proceed.

Best Practices for Employers

The SCA draws a firm line between company property and personal privacy. Employers can monitor their own systems, but accessing personal accounts—even if left open accidentally—can quickly cross the legal line and potentially lead to civil liability, exclusion of evidence in court or criminal penalties.

To ensure compliance with the SCA and avoid costly legal missteps, employers should adopt clear policies distinguishing between corporate and personal communications, train managers and IT personnel on SCA restrictions, and avoid accessing personal accounts without explicit written employee consent. By implementing these safeguards, employers can effectively protect both their business interests and their workforce's privacy rights. ■

If you would like more information about the SCA limits on accessing employee personal accounts, contact the NIEDWESKE LAW FIRM, LLC at 908-738-8500 and one of our highly skilled employment attorneys will assist you.