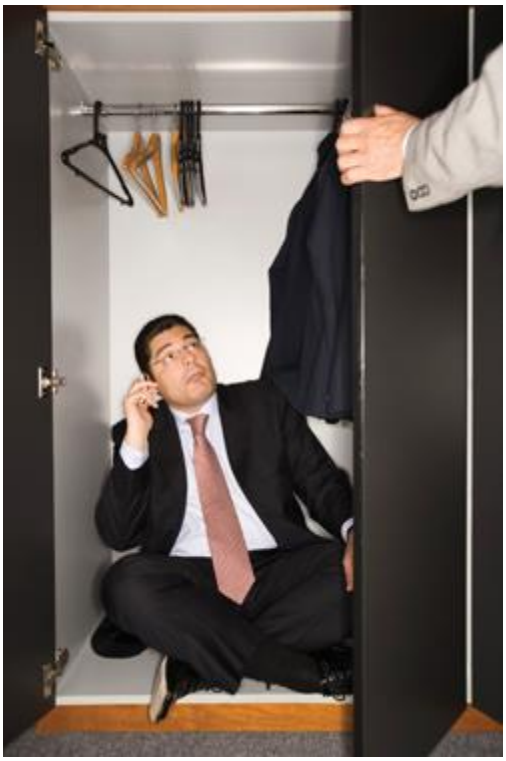
What Are the Limits of Employee Privacy?

Vol. 29 No. 6

ByDiane Vaksdal Smith, Jacob Burg

Diane Vaksdal Smith (dsmith@burgsimpson.com) is a shareholder with Burg Simpson Eldredge Hersh & Jardine in Englewood, Colorado, focusing on employment and appellate litigation. Jacob Burg (jburg@burgsimpson.com) is a second-year law student at the University of Denver and a law clerk with Burg Simpson.



Whenever a question arises about an employee's right to privacy in the workplace, it's best to start the analysis with the following question: What's the context? The answer is critical to identifying the rights that may be at stake as well as isolating the kind of technology being used. Public employees may have different rights than private employees. An employer's policies may eliminate an objective expectation of privacy. An employee may have a subjective expectation of privacy, based on the use of passwords, the segregation of information, or the equivalent of an electronic lockbox. Different forms of technology may simply not be treated as private.

It's also important to understand that the law regarding an employee's expectation of privacy has not yet caught up with all the forms of technology that are out there and can be used in a workplace. The existing law may not lend itself to analyzing claims dependent on electronic privacy. Many judges have declined to predict where the law is going because technology is changing so rapidly. For these reasons, privacy claims must be carefully evaluated on a case-by-case basis within the boundaries of the workplace.

Is there a right of privacy in the first place? There could be. An employee of a governmental employer may have a constitutionally protected reasonable expectation of privacy arising out of the Fourth Amendment. The Fourth Amendment doesn't apply to a private employer's property, on the other hand, when it comes to the relationship between employer and employee. However, there are still common law bases for a privacy interest, such as the common law claim for intrusion on seclusion. Both of these theories essentially require

the same thing: a determination of whether the employee's expectation is objectively and subjectively reasonable.

Because there are so many different work environments, each claim of privacy has to be evaluated based on the actual conditions of the workplace. Factors to look at include the use of the same office or piece of technology for a long time, the exclusive use of the space or technology, and the storage of personal items or information with the employer's knowledge, consent, or tolerance. The existence or lack of a policy, as discussed below, is also a consideration.

What do the employer's policies say? Express, comprehensive written policies can defeat an employee's expectation of privacy when it comes to the use of workplace technology because the continued belief in privacy after notice is not objectively reasonable. Consider whether the employer has a policy banning personal or other objectionable use of the computer or e-mail system, whether the employer monitors the use of the employee's computer or e-mail, whether third parties can access the computer or e-mails, and whether the employer notified the employee or the employee knew of the monitoring policies. In addition to policies, the employer could have a "pop-up" warning that appears when the computer is turned on or the e-mail system is accessed that expressly warns the user about the lack of privacy and the employer's right to monitor. All these are evidence that could defeat an employee's claim of an expectation of privacy.

What does the employer do to carry out the policies? An employer that fails to adopt policies or warnings or acts inconsistently with its policies or warnings may find that the employee still has a reasonable expectation of privacy. For example, adopting a policy that says "communications on the company e-mail systems are not private or secure" but then allowing an employee to use the e-mail system for personal business and prohibiting anyone but the employee from accessing a computer or e-mail system may lead an employee to expect privacy despite the policy. This could affect either the objective or subjective expectation of privacy.

Does the employee's conduct show a subjective expectation of privacy? Assume the employee signed off, showing receipt of the employer's policies that clearly state no privacy. Why would the employee continue to believe in a right of privacy after that? It could be that the employer acted inconsistently with the policies. It might also be that the employee took steps to limit access to information contained in the employee's workspace or technology. The employee may lock the office door or the desk drawer. The employee may password-protect the computer or encrypt e-mails. The employee may download and store information on an external device and store it away. Such conduct, particularly if unchallenged by the employer, can support a subjective expectation of privacy.

What form of technology is the employee using? Is the employee using GPS? Text messages? A cell phone? A computer? If the technology being used provides no more information than what is publicly available, then the employee probably can't reasonably have an expectation of privacy. A GPS device can track the location of a vehicle as it moves around—so do cameras and the human eye. It's unlikely that there is any expectation of privacy for an employee driving around in a company vehicle being tracked by GPS. This is consistent with criminal law concepts of privacy, where there is generally no expectation of privacy when a private vehicle is used to drive from one place to another. The fact that any passerby can observe where a vehicle is driving on the road or where it is parked militates against an expectation of privacy.

A text message is generally a private communication between the sender and the receiver. However, if the phone or computer on which the text message is sent belongs to the employer, then even assuming there is a right to privacy, the employee's expectation of privacy may have to give way if the employer has a legitimate purpose in searching an employee's phone or computer where the message was received. The employer may want to know if limitations on a company data or phone plan need to be increased to accommodate the number of users in the system or verify whether the employee has engaged in some kind of wrongful conduct.

E-mails are a widespread means of communicating, and employees may use the employer's e-mail system to communicate about personal matters to third parties. An e-mail sent on the work e-mail system will, in all likelihood, "belong" to the employer, and the employee should not have an expectation of privacy even if the subject matter of the e-mail is private. Unlike information stored on a computer hard drive, external hard

drive, or paper copy, the employer can access its own e-mail servers and the information contained there. Further, the employer can access the archives or backup of the e-mail servers.

E-mails sent or received on a company phone are also likely to be the "property" of the employer and subject to inspection and review, just as e-mails sitting in the in-box or out-box.

An e-mail on a private account, if used for the employer's work or saved to the employer's system, can probably be reviewed by the employer as well. However, if an employee views but does not save a private e-mail, the employee probably has a legitimate expectation of privacy.

Instant-messaging transcripts of conversations involving one or more employer-owned computers most likely belong to the employer for the same reason as the e-mails do and can be accessed under the same conditions.

What about an employee's right of privacy in social media? This is a tough one—yes, tougher than the others. At present, there is no general trend on the part of courts or legislators that address this issue, although there are discussions going on and possible legislative action.
If the employee's information is posted on a social media site without any safeguards—in other words, available to anyone who wants to look—then there isn't any reasonable expectation of privacy. If the employee's information is locked down and unavailable to the general public, then presumably it should be treated as private.
What are the trends for the future? Courts have been reluctant to adopt wholesale a new framework for analyzing employee privacy as it relates to developing technology, fearing that too much elaboration could lead to unpredictable future implications, particularly with the advent of smartphones, tablets, and other technologies we haven't seen yet. The Supreme Court recently had an opportunity to establish a framework for analyzing the extent of employee privacy in relation to text messaging on employer-owned devices, but the Court largely avoided making any new substantive law and instead analyzed the case using relatively old common law principles on privacy.

The courts are expected to hear more cases in the near future dealing with employee discipline for making negative comments about a supervisor or business on Facebook. We can only hope these cases lead to the development of new legal principles for analyzing and predicting the extent of an employee's right to privacy on social network sites.

Until that happens, claims about an employee's right to and expectation of privacy in new technologies will likely hinge on established common law principles to determine if the employee has a reasonable expectation of privacy and whether or not a search was reasonable. Because the courts will look to company policies, procedures, and conduct as a first step, it is important for employees to make sure that they have read and understand the employer's policies regarding the use of any technological medium. Courts have suggested that employees may maintain a reasonable expectation of privacy as it relates to personal e-mail and social network passwords, even if such media are accessed at work where passwords are stored on an employer's database. Employees need to be aware of the need to separate work and personal e-mails, as well as other forms of technology. Second, employees need to understand why the employer reserves the right to monitor and review e-mails, texts, and the like. An employer has a legitimate right to protect the workplace and the systems being used. In fact, some laws, such as those preventing workplace harassment, virtually require such monitoring. If the employer's conduct is reasonable, courts will almost certainly uphold the action.

We also need to watch for any legislative solutions. Several U.S. senators have questioned whether certain employer conduct—such as asking for a password to a social media site—violates existing law, and, if not, whether new laws should be put in place. At least one state legislature is considering a bill to protect employees from an employer's request for passwords.

This area of the law is in a constant and unpredictable state of development, and the employee's safest bet is to establish and keep a clear line between personal and private technologies in order to preserve any right to

privacy that might exist. If there's any doubt about whether some piece of information will remain private, assume that it will not and then decide whether it's something that should be out in the open.