Who Owns Business Data on Personally Owned Computers

Blurring boundaries between what is work time and equipment and what is personal time and equipment bring into question the ownership of information created on personal computers. What rights do employers have to access employee-owned computers used for work purposes? What expectation of privacy do employees have to personal information on employer-owned computers? A well-structured information policy can clarify the access and privacy rights of all parties.

John C. Montaña, J.D.
The intersection of an employee’s personal and work life and responsibilities has long been a difficult subject area for both employee and employer. This tension has increased over time as longer work hours and greater demands on employees make for an ever-longer workday. Often, it also means that employees work at home in the evening and on weekends.

In many cases, this work is done on a computer provided by the employer for the purposes of facilitating the employee’s at-home work. In many other cases, however, the work is performed on a computer owned by the employee or by someone else living in the employee’s residence. If the employee is doing substantive work on the employer’s behalf from such a computer, employee and employer may at some point find themselves in an adversarial position. The employer may expect or assume that it has some property right to at least some of the computer’s contents, while the employee may assume that contents on a personally owned computer is his or hers in its entirety and that the employer has no right of access to it.

**Privacy Law Governs Rights of Access**

Rights and access to potentially personal computer data is a topic that falls under the general rubric of “privacy.” Privacy law is a complex and often poorly defined combination of common law doctrines, constitutional law, and statutes and regulations. Much of this law is general privacy law and pre-dates computers; but increasingly, both statutory law and case decisions are directly on the topic of computer privacy.

Under the common law in the United States, invasion of privacy is a tort, for which the wronged party may seek compensation (Restatement, Second, of the Law of Torts, § 652B).

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

This statement is illustrative of the most common formulation of any common law wrong – the standard of conduct in most cases is that of what a “reasonable person” would do/think/expect in that particular situation. It is also illustrative of the continuing conundrum of privacy law, in general, and of computer privacy in particular: If a person believes that he or she has a privacy right or would be offended by an intrusion, such a right may exist if those expectations are consistent with the expectations of the hypothetical reasonable person whose actions and expectations are the plenary standard of the common law. In practice, that reasonable person is the judge or jury hearing the case.

Canada offers a different common law landscape. In contrast to the United States, a general common law privacy right has never been recognized or enforced by the courts. Recently, however, Canadian courts have begun examining this question and edging closer to recognition of a general right of privacy. In *R. v. Dyment*, the Canadian Supreme Court stated that privacy is “essential for the well-being of the individual.” In *Roth v. Roth*, an Ontario court found the basis for a right of privacy in the Charter of Rights and Freedoms. These cases, however, have never fully articulated an actionable general right of privacy. Thus, the nature of and the sources for a “reasonable” expectation of privacy will necessarily be different.

**Reasonable Expectation of Privacy May Limit Access**

A long line of decided cases (e.g., *TGB Insurance Services Corp. v. Zieminski*) makes clear that, in the absence of other factors, anything on an employer-owned computer system located on employer premises is properly the property of the employer and that the employer has a right of access at any time.

There are, however, factors that might give rise to such a privacy expectation. One such factor is an explicit employer grant of privacy, such as a personnel or information policy stating that the employer will limit its review or monitoring of employee communications or data on its systems. In such a case, the explicit grant of privacy presumably operates as an enforceable contractual provision. However, even in a case such as this, an employee privacy right that trumps all other considerations is by no means assured. If, for example – as in *Shoars v. Epson America, Inc* – the information over which a privacy right is asserted is communicated to another party over an employer-owned e-mail system, any right of privacy arising out of an explicitly stated e-mail privacy policy may be lost.

Another is an employer course of action implicitly granting the employee some privacy. This could be the allocation of “private” or “personal” folders on a computer system, or even merely acquiescing to or tolerating, even implicitly, the creation and maintenance of these folders on the employer’s system. Thus, for example, one Canadian court, in *Pacific Northwest Herb Corp. v. Thompson*, found an employee right of privacy in an employer-owned computer located at an employee’s home because the employee presumably had authority to use a com-
Computer at home for personal purposes even if such authority had never been explicitly granted. In an American case, *Leventhal v. Knapek*, a right of privacy was found merely because of the physical layout of the office:

[The employee] occupied a private office with a door. He had exclusive use of the desk, filing cabinet, and computer in his office. [The employee] did not share use of his computer with other employees in the Accounting Bureau nor was there evidence that visitors or the public had access to his computer.

It is important to note, however, that the finding of a right of privacy enjoyed by the employee does not necessarily equate with an ability by the employee to prevent employer access. In each case, a balancing test is applied. The courts come to highly fact-dependent conclusions, and outcomes are not always consistent. However, the common thread in them is that the courts attempt to arrive at a determination of whether the course of dealings between the parties gave rise to an expectation of privacy that would have been held by the hypothetical reasonable person. Far more often than not, the employer prevails, regardless of a hypothetical privacy right that might be asserted against some outside party.

**Computer Ownership Is Key Factor**

Decided cases on employee computer privacy are, in many cases, inapt for this discussion because they assume a clear-cut boundary between work and home environments – or at least between employer-owned computers, upon which all work is assumed to have occurred, and home computers, which are not usually assumed to have been involved in the work process. At some point in the past, and in many instances today, this bright-line distinction may be valid.

In many cases, however, these distinctions are not valid. Employer work is commonly done on otherwise clearly private premises, and a given item of work may be worked upon on two or more

machines owned by the employer, employee, and others, with multiple copies of the work item residing in these places in various versions and states of completion.

It is clear, however, that ownership of the computer system upon which the data resides is an important factor in decided cases. The usual rationale for not finding an employee privacy right on an employer-owned computer system is usually a variation on the proposition that the owner of a system or piece of equipment does not need permission to inspect any part of it for any reason or no reason. One Canadian court, in *Zesta Engineering Ltd. v. Cloutier*, stated the general doctrine thus:

While it may be, as his counsel asserted, that [the employee] had a reasonable expectation of privacy regarding what was on his work computer, that belief in privacy does not change the fact that [the employer] could access the computer when it wanted to without the need of a court order.

U.S. courts have been similarly reliant upon employer ownership as a decisive factor in finding the absence of a privacy right. Ownership of the system upon which the information resides or is transmitted has also proven an effective defense against statutory protections against eavesdropping, wiretapping, or other interceptions or unauthorized viewings of electronic data. In discussing a right of privacy allegedly attaching to e-mail in *Shoars v. Epson America, Inc*, one court stated:

We do not construe the [a provision of law prohibiting eavesdropping on or recording confidential communications] as rendering e-mail messages sent or received as part of [the employer’s] business confidential as to [the employer] itself.

Many laws restricting access to electronic data explicitly articulate a business-need or ownership exception to their prohibitions, and courts, among them the above-cited example, commonly conclude that electronic data privacy laws simply do not apply as against the owner of the system on which data resides, particularly if the employee was on notice of the ownership and of the possibility that the employer might for some reason peruse the data. In *Bouke v. Nissan Motor Corp. U.S.A.*, one court put it bluntly:

[The employer’s] actions in retrieving, printing and reading plaintiffs’ E-mail messages simply are not included within the actions proscribed by Penal Code section 631 [a California wiretapping law].

What courts have thus far failed to articulate, but which stands as a corollary to this doctrine, is that if the computer is owned by the employee and the data in question never migrated to an employer-owned system, the expectation of privacy on the part of the employee is correspondingly higher. At the very least, the doctrine of employer ownership and its core tenet that the
The often amorphous rights and expectations of the common law are supplemented by a very wide variety of privacy rights – often narrow in scope and highly situational – granted by statutory enactment. Potentially relevant enactments are below.

**United States**
- *The Electronic Communications Privacy Act (ECPA)* protects electronic communication generally.
- *The Cable Communications Policy Act (CCPA)* in effect supplements the privacy expectations above by placing a cable provider in the position of being a third party expected to enforce a privacy expectation on behalf of a consumer.
- *The Economic Espionage Act (EEA)* criminalizes theft of trade secrets, even in cases where no physical objects are taken. This, to some extent, counters the effects of ECPA and CCPA. To the extent that the employee’s computer may contain work product owned by the employer, the employer may be able to assert a property right in it and thereby gain access to the employee’s computer and its contents.

**Canada**
Although Canada recognizes no common law privacy right, it has three general overall privacy laws in place. These enactments are much broader than their U.S. counterparts, therefore mitigating or eliminating the absence of a common law right. Further, because they are quite broad and non-situational (as compared with the U.S.’ topic-by-topic and service-provider-by-service-provider approach to privacy law), Canadian employees are far less likely to find themselves with no privacy right whatsoever due to the particular characteristics of data delivery or the identity or market niche of a service provider.
- *The Canada Personal Information Privacy and Electronic Documents Act (PIPEDA)* is an implementation of the Data Privacy Directive (adopted by the European Union [EU] and binding upon all EU states, Hong Kong, Russia, and a number of other jurisdictions), sets forth ground rules for how organizations can collect, use, or disclose personal information in the course of commercial activities.
- *The Privacy Act* was enacted “to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.”
- *The Criminal Code (Part IV)* gives rise to an expectation of privacy in electronic data by making willful interception of a private communication by means of any electro-magnetic, acoustic, mechanical, or other device a criminal act. It thus operates in much the same manner as Title 1 of the U.S.’s ECPA.
Key Questions in Determining Rights of Access to Data

Regardless of the data on an employee-owned computer and rights of access to and ownership of it, the positions of the employee and employer are essentially adversarial. The employer would like to gain as great a right of access and as much ownership as possible while the employee would like to limit that access and ownership to the greatest extent possible. The following questions are relevant:

- **Who owns the physical equipment on which the data is stored?** If the employer owns the physical equipment and system, there is little doubt that the employer has at least a right of access to data on it. The corollary is no doubt equally true – employee ownership of the computer will be strongly indicative of employee control of the data on it.

- **Has the data been transferred to the employer’s system or to third parties?** Even if the data originated on the employee’s own system, transfer of the data to the employer’s system or to a third party may reduce or eliminate any privacy right that the employee may initially have had.

- **How have the involved parties dealt with this issue in the past?** If the employee has had reason to believe that the employer would access the data or that the employer retained the right to do so, particularly if the employee has acquiesced to this arrangement, this may preclude the assertion of a privacy right. Conversely, to the extent that the employer has offered or acquiesced to an arrangement whereby the employee has a *de facto* privacy arrangement, this may give rise to a reasonable privacy expectation.

- **What are the statutory rights and privileges that apply to the data?** Any privacy law applicable to the data in dispute will be at least indicative of a privacy right and expectation that may be asserted.

- **Is there an information management policy in place?** The terms and conditions of such a policy may be controlling in a dispute.

- **Did the employee sign an intellectual property agreement?** To the extent that such an agreement is broad, it may permit a credible claim of ownership – and thereby access – to a great deal of the data stored on a personally owned machine.

- **How is the data arranged on the computer?** If employer data is segregated from other data in separate directories or other data structures, this may be indicative of the assertion of an expectation of privacy in other material. In similar manner, password protection, encryption, and other protective devices may be indicative of an expectation of privacy. Conversely, co-mingling employer data with personal data may diminish the reasonableness of any privacy expectation, as may connecting the computer to an employer network or e-mail system.

the data, there may be a privacy expectation as against the employer.

In some cases, this issue is resolved in the employment agreement. In employing engineers, scientists, and others whose work may involve creation of marketable intellectual property, employers commonly require the employee to sign an agreement granting the employer rights to all intellectual property created during the term of employment. Such agreements, which are often written in sweeping language, give the employer an enforceable right of ownership in work-related data, regardless of its format, physical location, or ownership of the equipment on which it resides. If such an assignment has been made, as seen in *Self-Realization Fellowship Church v. Ananda Church of Self-Realization*, it is enforceable. However, in the absence of an agreement between employer and employee, ownership and property rights will undoubtedly be subject to the same sort of reasonableness test as has been described above.

**Strategies for Clarifying Rights of Access**

**Employee Strategies**

Most employees do not intend for their employers to have any right of access to or ownership of the contents on their employee-owned computers. At the least, any data relating to personal matters is undoubtedly viewed by most employees as entirely private. The employee’s goal is to give the employer neither the expectation of ownership of any other data nor any legal justification for perusing other data on the pretext of trying to find employer-owned data. Several steps can further this goal.

1) **Read policies and negotiate before signing.** The employee should carefully read and consider the language and import of any information or intellectual property ownership policy he or she may be asked to sign. If the language is unacceptably broad with respect to ownership, the employee should renegotiate the agreement and avoid subsequent actions that might be construed as broadening the rights granted by it.
2) Keep personal computers private. Actions on the part of the employee may be indicative of an expectation of privacy or of the lack of one. The employee should, therefore, carefully consider the implications of such things as:

- permitting other employees to access a personal machine and its data
- linking a personal computer to an employer network or keeping it on employer premises
- installing employer-owned software on a personal computer

3) Segregate and protect personal data. Employer data should be segregated from personal data by means of suitable data structures. If other employees have access to the machine or its environment, either physically or through a remote connection such as a network, personal data should be protected by file-sharing restrictions, passwords, encryption, or other security devices.

**Employer Strategies**

Although it may be tempting to further the employer’s ownership interests by creating a sweeping information ownership policy that gives the employer ownership of or access to anything on the employee’s personal computer, this may be counterproductive. Employees may respond by simply not engaging in employer business on their own equipment, reducing the productivity of those who would otherwise be willing to work outside of the regular business environment. Therefore, the employer’s approach must avoid heavy-handed policies or clearly unreasonable demands. The employer should consider the following:

1) **Determine the need for intrusive access policies based on the type of work being done.** What kind of data are employees actually sending home or creating there as part of their work-related activities? For some employees, a very intrusive policy may be required. In many cases, however, the data in question will be routine, easily replaceable, and relatively low-risk information such as reports and presentations. If so, an intrusive policy may not be necessary.

2) **Manage employee expectations.** Employees may well assume that they own a copy of employer data maintained on their personal computers. As part of its information policy, the employer should make clear that copies of employer-owned data remain the employer’s property regardless of who owns the media or equipment upon which the data are stored. If the employer has an information policy granting employees privacy rights in computer data (e.g., it permits the maintenance of personal folders on computers), it should make clear that the policy applies to particular data objects, such as personal documents, and not to employer data in general.

3) **Provide computers to employees for important offsite work.** If the employer relies heavily on work performed off-site by employees and if the resulting work product is of high value, it may be prudent simply to provide employees with laptop or home computers. From the employer’s perspective, this virtually eliminates the entire problem. Courts almost always side with the employer in cases where the employer owns the computer, particularly when this is combined with a clear information policy agreed to by the employee.

**The Value of a Well-Structured Information Policy**

Ultimately, the outcome of any privacy dispute between an employer and employee will be heavily influenced by the contents of the employer’s information ownership policy and evidence that the employee understood and agreed to it. This being so, it is in the best interests of both parties to ensure that such an agreement is in place, that its contents reflect the actual expectations and understandings of the parties, and that both parties agree to abide by its rules.

The absence of a policy, coupled with unspoken assumptions about ownership and access to data, is far more likely to result in disputes and litigation than any information policy itself. Such a policy, when combined with sound management of the data in question, will permit both parties to effectively further their joint goals, which is the purpose for having the data on an employee-owned computer in the first place.

**Editor’s Note:** This article is based on a study conducted with funding from the ARMA International Educational Foundation (www.armaedfoundation.org). The full results of the study are available in the report “Access Rights to Business Data on Personally-Owned Computers,” which is available through the ARMA International Bookstore (www.arma.org/bookstore).

---

**John C. Montaña, J.D.,** is a records management and legal consultant and principal of Cunningham and Montaña Inc. He may be contacted at johnmontana@qwestinternet.com.