ARMA International Educational Foundation

Access Rights to Business Data on Personally-Owned Computers

By

John C. Montana, J.D.

October 2004

Project Underwritten by:

The Houston and Calgary Chapters of ARMA International

in conjunction with

The ARMA International Educational Foundation Endowment Fund

1609 Terrie Drive
Pittsburgh PA 15241 USA

www.armaedfoundation.org

Access Rights to Business Data on Personally-Owned Computers

A White Paper by John C. Montaña
For
The ARMA International Education Foundation

1. Introduction

The intersection where an employee's personal life, work life and responsibilities meet has long been a difficult subject area for both employee and employer. This tension has increased over time as longer work hours and increased demands on employees require that employees spend time managing personal responsibilities from the workplace. This may require personal phone calls and e-mail, as well as the use of employer-owned computers for personal tasks and activities. For the employer, this personal use of equipment and time for personal activities poses several issues: time spent on personal activities decreases – at least in theory – the productivity of employees; should the employee engage in an activity that is improper or illegal, it may also place the employer at risk of being liable for the employee's actions.

In the workplace environment, the employer's array of responses to this set of issues is commonly thought to be clear and effective: ban or limit the employee's use of computers for personal use, and notify employees that workplace computers may be monitored to ensure that no inappropriate or illegal activities are occurring. Since the employer owns the computers in question, the employer is thought to have full access to any and all data on the computer, and the employee is thought to have no right to privacy in anything on it; nor any ability to assert a superior claim to ownership of any of its contents.[1]

The continuing and pervasive blurring of the boundaries between work and home environments is another reality for many workers. Increased responsibilities and workloads, demands for longer hours and many other factors combine to create a situation in which many workers are required to resort to extraordinary measures to meet the demands of work and profession.

In many cases, these demands are met by working at home. Increasingly, this work is computer-based work, and includes e-mail, word processing documents, spreadsheet and other computer-generated data objects. 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 the employee themselves or someone else living in the employee's residence.

It may well be that ownership and control of data is vested in the employer in the workplace environment, or of computers owned by the employer. However, this assertion is less obviously true of computers not owned by the employer or located on the employer's premises. If the employee is doing substantive work on the employer's behalf from such a computer, a tension is thus created: the employer may expect or

[1] See, e.g., *Employee Privacy -- Computer-Use Monitoring Practices and Policies of Selected Companies*, United States General Accounting Office Report to the Ranking Minority Member, Subcommittee on 21st Century Competitiveness, Committee on Education and the Workforce, House of Representatives, Sept 2002, indicating the a majority of surveyed companies reviewed employee e-mail when violations of company policy were suspected.

assume that it has some property right in at least some of the computer's contents, while the employee may assume that a computer owned by them is theirs in its entirety, and that the employer has no right of access to it or any of its contents. If some of those contents are perceived by the parties to be valuable, this tension may be considerable.

1.1. The Issue

What, then, are the rights of the parties in this situation? Can the employer demand access to the contents of a computer owned by the employee and located someplace other than employer premises? Can the employee deny the employer access to any and all of the data on such a computer, even if the employer has reason to believe that some of that data either belongs to the employer or affects the employer's rights or responsibilities?

1.2. This Paper

This paper seeks to examine these questions and determine what the rights of the respective parties are, based upon current law and legal trends. It will also set forth the factors, both legal and practical, upon which those rights are based. It will then set forth some suggested practices for both employee and employer that will help clarify both the rights and expectations of the parties.

The reader should beware: This is an area of law with many grey areas, and with many undecided issues. No statutes are directly on point, and past cases focus exclusively upon employer-owned computers and systems. Expectations and course of dealings between the parties may heavily influence the outcome in any particular case, as may the idiosyncrasies and inclinations of the judge before whom a case is heard. Both employer and employee should proceed cautiously and prudently, and not make assumptions about ownership of data.

2. Privacy

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 area of law. It is a combination of common law doctrines, constitutional law, 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.

> 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.[2]

[2] Restatement, Second, of the Law of Torts, § 652B

This statement of the common law 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: the existence and scope of a right of privacy is determined in many cases in large part by the expectations of the parties. If a person believes that they have 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. What then, we may ask, are the expectations of the reasonable person, and what factors may either influence them or alter them?

2.1. The Expectation of Privacy: Where It May Arise

2.1.1. Constitutional and Implied Rights

The expectations of the reasonable person postulated by common law are overlain on a very substantial substrate of other law. There are, for example, constitutional provisions relating to privacy. They may be explicit, as in California:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.[3]

They may also be implicit, as in the United States Constitution, wherein the United States Supreme Court has found limited privacy rights with respect to governmental action implicit in the Fourth Amendment[4] and which have been made applicable to the states via application of the 14th Amendment.[5]

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, they have begun examining this question and edging closer to recognition of a general right of privacy. In one case, the Canadian Supreme Court stated that privacy is "essential for the well-being of the individual."[6] An Ontario court has found the basis for a right of privacy in the Charter of Rights and Freedoms.[7] These cases, however, have never fully articulated an actionable general right of privacy. Thus, the nature of a "reasonable" expectation of privacy will necessarily be different, and the sources for any such expectation will necessarily be different.

2.1.2. Privacy and Expectations

[3] California Constitution, Art. 1 § 1.
[4] *See, e.g., Katz v. United States*, 389 U.S. 347 (1967).
[5] "[N]or shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."
[6] *R. v. Dyment*, (1988) 2 S.C.R. 417.
[7] *Roth v. Roth* (1991), 9 C.C.L.T. (2d) 141 (Ont. Gen. Div.).

In view of the above, the question of expectations looms large in any resolution of the issue of employer access, since expectations, if they are those of a reasonable person, may give rise to a privacy right.

2.1.3. The Absence of a Reasonable Expectation

A long line of decided cases 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.[8]

There are, however, factors which 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, 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.[9]

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 in or tolerating, even impliedly, the creation and maintenance of them on the employer's system. Thus, for example, one Canadian court found an employee right of privacy in an employer-owned computer located at the employee's home, because the employee presumably had authority to use a computer at their home for personal purposes, even if such authority had never been explicitly granted.[10] In an American case, a right of privacy was found merely because 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.[11]

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.

---

[8] *See .e.g., TGB Insurance Services Corp. v. Zieminski*, No. B153400 (Cal. 2nd App. Dist 2002) (unpublished opinion).
[9] *See., e.g., Shoars v. Epson America, Inc.,* No. B 073234 (Cal. App. 2nd Dist. 1994) (unpublished opinion).
[10] *Pacific Northwest Herb Corp. v. Thompson* (1999) B.C.J. No. 2772 (B.C.S.C.).
[11] *Leventhal v. Knapek*, 266 F.3d 64 (2nd Cir. 2001).

2.1.4. Statutory Rights Which May Give Rise to an Expectation of Privacy

A factor that may give rise to a privacy expectation is the existence of a law granting a privacy right in some data set or in some set of circumstances. The existence of such a law may be of considerable importance when, as is often the case, the parties are silent as to their respective expectations, and may be operating under radically differing assumptions concerning ownership and access to the data stored on a personally owned computer.

2.1.4.1. The United States

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. Among the potentially relevant enactments are:

The Electronic Communications Privacy Act,[12] (ECPA), which protects electronic communication generally. It is broken into two titles: Title I deals with the unauthorized and intentional interception of transitory electronic communications.[13] Title II deals with intentionally gaining access to stored communications without authorization.[14] Collectively, these provisions have several effects germane to this discussion:

First, they establish a privacy right in electronic communications, and in electronic records of those communications. This establishes a legal basis upon which to assert a privacy interest or privacy expectation.

Second, they prohibit the use of intercepted communications as evidence in legal proceedings.[15] If the employer is seeking access to material on an employee-owned computer due to a legal dispute, or a dispute which may end up in court, any material from it obtained by unauthorized means may be valueless to the employer.

Third, the prohibitions in ECPA include third parties such as ISPs, who are prohibited from providing anyone -- including an employer -- access to material in the third party's possession to which the employee's privacy right attaches.[16]

Collectively, these provisions establish a possessory and privacy right that may be asserted by an employee. Third parties who may have access to the information must also assert that right on behalf of an employee or risk penalties, thus both further limiting the employer's access and reinforcing the perception of a privacy right.

The Cable Communications Policy Act,[17] (CCPA), which 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. If the employee receives internet service via cable modem, this may be an additional factor in asserting a

[12] 18 U.S.C. § 2510 *et seq.*
[13] 18 U.S.C. § 2511.
[14] 18 U.S.C. § 2701.
[15] 18 U.S.C. § 2515.
[16] 18 U.S.C. § 2702.
[17] 47 U.S.C. § 551 *et seq.*

privacy expectation, and an additional obstacle to employer access under some circumstances.

The Economic Espionage Act,[18] (EEA) which criminalizes theft of trade secrets, even in cases where no physical objects are taken. This has an effect which 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 -- particularly if the employer can credibly claim that the information is a trade secret or other intellectual property -- the employer may be able to assert a property right over it, and thereby gain access to the employee's computer and its contents.

2.1.4.2. Canada

Although Canada recognizes no common law privacy right, Canada has two general overall privacy laws in place. Both enactments are much broader than any of their United States counterparts, therefore mitigating or eliminating the absence of a common law right. Further, since both are quite broad and non-situational (as compared with the United States' topic-by-topic and service-provider-by-service-provider approach to privacy law), the Canadian employee is far less likely to find herself 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,[19] an implementation of the Data Privacy Directive,[20] and which sets forth ground rules for how organizations can collect, use or disclose personal information in the course of commercial activities.

The Privacy Act,[21] 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."[22]

The Canadian legislation is enforced by a governmental body, the Office of the Privacy Commissioner. There are in addition, general data privacy laws in the provinces, as well as privacy commissioners. These laws have the effect of adding redundant layers to the expectation of privacy found in the national legislation.

The Criminal Code. In addition the above, an expectation of privacy in electronic data arises from Part VI of the Criminal Code,[23] which makes 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 ECPA.

---

[18] 18 U.S.C. § 1831 *et seq*.
[19] Second Session, Thirty-sixth Parliament, 48-49 Elizabeth II, 1999-2000, bill C-6.
[20] Adopted by the European Union and binding upon all of the states within that Union, Hong Kong, Russia and a number of other jurisdictions.
[21] R.S. 1985, c. P-21.
[22] Id., § 2.
[23] § 184(1).

Canadian commentators and at least one court[24] have concluded that, in determining the expectations of the parties, reference to statutory law and the expectations it creates is appropriate.

2.1.5. Ownership and Expectations

Decided cases on employee computer privacy are, in many cases unsuitable for the purposes of this discussion, in that 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. Decided cases have also focused on the ownership of the computer equipment itself, and not on ownership of the data in question.

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 edited 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 completeness.

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 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.[25]

United States 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, 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.[26]

Many laws restricting access to electronic data explicitly articulate a business-need or ownership exception to their prohibitions, and courts, among them have cited the above

[24] *McLeod v. Egan* (1997), 46 D.L.R. (3d) 150.
[25] *Zesta Engineering Ltd. v. Cloutier*, 2000 Carswell Ont. 1065.
[26] *Shoars v. Epson America, Inc.*, No. B 073234 (Cal. App. Dist. 2 1994) (unpublished opinion).

example, commonly conclude that electronic data privacy laws simply do not apply as against the owner of the system on which data reside, particularly if the employee was on notice of the ownership, and of the possibility that the employer might for some reason peruse the data. 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). [27]

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 migrate 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 employer's ownership of a system trumps virtually all other considerations, is inapplicable, along with the body of case law standing for that proposition.

2.1.6. Contractual Expectations

Business organizations, particularly large ones, commonly have employees read and agree to information policy statements that create a diminished or absent expectation of privacy in workplace communications and data. They do so by placing the employee on notice that the employer grants no privacy rights on its computer system, and reserves the right to monitor or inspect all data and transmissions on the system. Courts are in agreement that such notices or agreements may substantially govern any privacy rights that an employee may have. In rejecting one employee's claim of a privacy right, one court analyzed it thus:

> [The employee] signed [the employer's] policy statement, thereby acknowledging his understanding that the home computer was "the property of the Company" and, as such, "to be used for business purposes only and not for personal benefit or non-Company purposes." . . . His signature shows that he read the Company' s policy, understood it, and agreed to adhere to it.
>
> As can be seen, [the employee] knew that [the employer] would monitor the files and messages stored on the computers he used at the office and at home. He had the opportunity to consent to [the employer's] policy or not, and had the opportunity to limit his use of his home computer to purely business matters. . . . With all the information he needed to make an intelligent decision, [the employee] agreed to the Company' s policy and chose to use his computer for personal matters. By any reasonable standard, [the employee] fully and voluntarily relinquished his privacy rights in the information he stored on his home computer, and he will not now be heard to say that he nevertheless had a reasonable expectation of privacy.[28]

---

[27] *Bouke v. Nissan Motor Corp. U.S.A.*, No. B068705 (Cal. App 2nd Dist 1993) (unpublished opinion).
[28] *TGB Insurance Services Corp. v. Superior Court*, supra.

Commentators are in agreement that the existence of such a policy, disseminated to the employee, is a key factor in deciding privacy rights in an employment situation.[29]

2.1.7. Ownership of Data

In the typical formulation, the employer's information policy statement contains language that the employer owns the computer system and all data upon it. This language begs the question of data created by the employee in furtherance of the employer's business purposes, but which never actually migrates to the employer's computer system. If such data is owned by the employer, any privacy expectation with respect to it on behalf of the employee may be substantially diminished if not entirely eliminated. If, on the other hand, the employee owns it, 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:

> The employee agrees:
> (a) that all inventions and improvements made, developed, perfected, devised, or conceived by the Employee either solely or in collaboration with others during the Employee's employment by [corporate name], whether or not during regular working hours, relating to the business, developments, products, or activities of [corporate name], or its subsidiaries, shall be and are the sole and absolute property of [corporate name]; and to disclose promptly in writing to [division name]'s Legal Department or to such other person as [corporate name] may designate, such inventions and improvements.[30]

If such an assignment has been made, it is enforceable.[31] For most employees, however, any information policy agreement -- if there is one -- is unlikely to contain such language. There are apparently no decided cases affirmatively answering the question of who owns a document created by an employee in furtherance of work-related duties, but which never gets migrated onto an employer-owned system. Thus, 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. There is, in this case as in other cases, a spectrum of cases to which such a reasonableness test might apply.

---

[29] *See, e.g.*, Samuels, Melanie C. and Gregory, Sara; *Privacy Issues in the Workplace: Employer Monitoring of Employee Technology Use; 2001* (discussing Canadian law); Ravin, Richard L., and Halpern, Steven E., *Employee and Student Privacy Interest In The Computer Age*, New Jersey Lawyer Magazine (August 1999).

[30] From Laney, Orin E., *Intellectual Property and the Rights of Creative Employees* (1999), www.cerebraltrespass.com/ipguideweb.htm#A, for which see a more general discussion of this issue.

[31] *See, e.g., Self-Realization Fellowship Church, v. Ananda Church of Self-Realization*, 206 F.3d 1322 (9th Cir. 2000)

At one end of the spectrum, a document clearly owned by the employer (e.g., generated on the employer's data systems, and perhaps thereby subject to intellectual property or trade secret laws) is copied and transmitted to some other computer. In such a case, the document in question is a duplicate of something already owned by the employer, and as such may well be controllable by them under existing intellectual property or other law.

Beyond this point, however, things are very much less clear. If the employee revises the document on non-employer equipment or premises, whose property is the revision, and the intellectual capital behind any such revision? If the document or data is created entirely on non-employer equipment and premises, and merely relates to employer business -- regardless of the value it might ultimately have to the employer -- does the employer have any rights whatsoever in it?

There appears to be very little legal guidance in this area. Decided law focuses on ownership of the computer system itself, and emphasizes that the employer may *access* information on the system, without actually addressing the question of *ownership* of the data. The question of ownership may, therefore reduce itself to the relationship the parties have built, and the expectations arising out of that relationship. It may well be, however, that in absence of a clearly communicated agreement on employer ownership, the employer may have little right to such data.

2.2. The Formulation of a Privacy Expectation

When considering the question of data on an employee-owned computer, and the respective rights of access 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. In particular, the employee would like to be able to assert an effective privacy right in any material that may reside on the computer that is not directly related to the employer's business.

Considering these positions in light of statutory law and decided cases, it is possible to articulate the points that each party must bear in mind.

Ownership of the physical equipment on which the data is stored. Past cases focus heavily on ownership of the computers which contain the data in question. If the employer owns the physical equipment and system, there is little doubt they have at least a right of access to data on it. Although past cases focus on employer ownership and the rights arising out of 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.

Transfer of data to the employer's system or to third parties. Even if the data originate 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 which the employee may initially have had. Some third parties such as ISPs may be bound by privacy law, but many are not, and the employer may well be able to gain access to the information from them, regardless of whether access to the employee's computer is gained. This may be so even if the data sought would otherwise have clearly had some legally enforceable privilege such as attorney-client privilege attaching to it.

Past course of dealing between the parties. 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 in an arrangement whereby the employee has a *de facto* privacy arrangement, this may give rise to a reasonable expectation of privacy on the part of the employee. In the case of a computer owned by the employee, and for which the employer has no default right of access, the course of dealing may be particularly significant.

Statutory rights and privileges in 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. Further, to the extent that such laws obligate third parties such as ISP's or cable companies to protect data privacy, they may serve to prevent an end-run by the employer, should be employer seek to by-pass the employee and her computer entirely and attempt to obtain the data from these third parties.

The presence and precise wording of any employer information management policy. In such a policy, the employer typically claims ownership of some data set. The precise data set so defined may be very important. A right of ownership may permit the bootstrapping of a right of access, and thereby in turn perhaps a right of entry onto the employee system and access to other data thereon.

The presence and precise wording of any employer intellectual property agreement. Such agreements may be quite broad, and encompass any intellectual property of any kind developed by the employee at any time during the term of employment, or they may be quite narrow, dealing only with specified kinds of intellectual property, or have other limitations on the ownership claimed by the employer. 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 upon a personally owned machine.

Physical arrangements on the computer itself which would indicate that the employee is asserting a privacy right to it and its contents. 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 hooking up the computer to an employer network or e-mail system.

It is important to note that in no case is any one of the factors above necessarily dispositive of the existence of an enforceable privacy expectation. When looking at the case, a court will weigh the total mix of these and other factors, and make a determination based upon an evaluation of the total set of facts and circumstances. In formulating a strategy for dealing with data privacy, both employer and employee should bear in mind that a court may give greater weight to some factors than others, and may do so in a manner that does not agree with their own notions of what factors ought to weigh most heavily.

3. Strategies and Tactics for the Parties

3.1. The Employee

Most employees do not intend for their employer to have any right of access or ownership in the contents of the employee's own computer. Even assuming that the employee is willing to concede ownership of work-related data on the computer to the employer, any data relating to personal matters is undoubtedly viewed by most employees as entirely private. The employee's goal in this case is to give the employer neither the expectation of ownership in 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.

Communication. Since courts rely heavily on any agreements the parties may have entered into regarding data ownership and access, the employee should carefully read and consider the language and import of any information or intellectual property ownership policy she may be asked to sign. If the language is unacceptably broad with respect to ownership, or appears to give the employer a right of access to data, data structures or physical locations or equipment that the employee is unwilling to grant, the employee should re-negotiate the agreement. Thereafter, the employee should guard against making any statements which can be construed as a grant of ownership or access to these things. If it is politically possible for the employee to do so, she may wish to formally notify the employer that she grants no right of access or ownership to data contained on a personal machine.

Course of dealing. 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 the machine and its data. This includes access for normal business purposes, and access by technical staff for maintenance, repair and similar activities.

- Linking a personal computer to an employer network, or keeping it on employer premises.

- Installation of employer-owned software on a personal computer.

Each of these, to the extent it is present, may diminish the reasonableness of any expectation of privacy. In particular, routine, unsupervised and uncontrolled access to data on the machine by other agents or employees of the employer may serve to drastically diminish any privacy expectation.

Data segregation. 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.

3.2. The Employer.

The employer has an interest in access and ownership to data created in furtherance of its purposes, regardless of the location of the data and the intent of the creator. Although it may be tempting further this interest 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, thus reducing the added productivity and additional hours of work the employer gains when employees are so willing. Therefore, the employer's approach must avoid heavy-handed policies or clearly unreasonable demands. This will necessarily demand that the employer consider the nature of the information itself, and the employer's real need for access to it. The employer should therefore consider:

Actual need. What kind of data are employees actual sending home or creating there as part of their work-related activities? For employees whose duties give them access to very valuable information such as intellectual property, or to data of a very sensitive nature, a very intrusive policy may be required, and will probably be understood by the employees in question as necessary. For other employees, however, the intrusiveness of the policy should be proportional with the actual need. In many cases, 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.

Managing employee expectations. Employees may well assume that a copy of employer data maintained on a personal computer is owned by the employee, since the employer still maintains their own copy. As part of its information policy, the employer should make clear that copies of employer-owned data remain the employer' property, regardless of the ownership of the media or equipment upon which they are stored, and that all such copies must be returned upon demand, including revised and altered versions of this data. The agreement should also clearly cover data created on a personal machine, if warranted. If the employee is subject to an intellectual property agreement, that agreement should cover the same matters. If the employer has an information policy granting employees privacy rights in computer data (i.e., 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 that actions such as placing employer data in a personal directory or on a personal machine do not make them personal data, or grant a privacy right with respect to them

Ownership of the computer. 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.

3.3. The Value of Data Segregation for Both Parties

Regardless of any privacy expectation that may exist, if a dispute between an employee and employer rises to the level of litigation, the employer will be able to gain access to information germane to the dispute, including information on the employee's computer, through legal process, regardless of other ownership or access rights. The question in that case is what information, and how easily?

From this perspective, co-mingling of business and personal data on the employee's computer is problematic for both parties. From the employee's perspective, a successful attempt by the employer to gain access to business data co-mingled with personal data (as through, for example, legal process coupled with forensic computer analysis) may result in the employer's gaining access to personal data they might otherwise never have seen. From the employer's perspective, the co-mingling may result in the assertion of a privacy right by the employee that might otherwise not have arisen, or at least would not have been as compelling; thereby complicating efforts to gain access to data the employer may have a legitimate right to.

The solution for both parties is to ensure that employer data is properly segregated, so that issues surrounding it are at least minimized, and possibly eliminated. For the employee, employer data can be handed off cleanly and easily, and with less suspicions that data is intentionally or unintentionally missing from the returned data set; for the employer, messy privacy disputes are avoided. For both, extended and expensive legal wangling is avoided. As a matter of self-interest, therefore, the employee should ensure that employer data resides in suitably structured directories or folders, with an appropriate level of protection. Equally as a matter of self-interest, the employer should encourage the same.

3.4. Conclusion: The Value of a Well-Structured Information Policy

Ultimately, the outcome of any privacy dispute between and 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.

In agreeing to such a policy, the parties should take into account the legitimate interests of the other party. For the employee, this means understanding that the employer has a legitimate ownership interest in its business data, and the right to protect and manage that data in a manner consistent with its business needs. For the employer, this means understanding that the employee has a legitimate interest in keeping her personal affairs and data private. Such a policy, combined with sound management of the data in question, will permit both parties to effectively further their joint goals, and that, after all, is the purpose for having the data on an employee-owned computer in the first place.

Bourke v. Nissan Motors

THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION FIVE

No. B068705

BONITA P. BOURKE et al.,

Plaintiffs and Appellants,

v.

NISSAN MOTOR CORPORATION IN U.S.A.,

Defendant and Respondent.

July 26, 1993

APPEAL from a judgment of the Superior Court of Los Angeles County. Douglas A. McKee, Judge. Affirmed.

1) Plaintiffs Bonita Bourke and Rhonda Hall appeal the entry of summary judgment in their suit against Nissan Motor Corporation in U.S.A. ("Nissan") alleging wrongful termination, invasion of privacy and violation of their constitutional right to privacy in connection with Nissan's retrieval, printing and reading of E-mail messages authored by plaintiffs.

We affirm.

FACTS

2) Plaintiffs were hired by Nissan in June of 1989 as Information Systems Specialists, to assist Infiniti car dealership personnel in resolving problems with the computer system which ran the operations of Infiniti dealers. Plaintiffs were essentially customer service representatives for users of the computer system.

3) In June of 1990, one of plaintiffs' co-workers, Lori Eaton, was conducting a training session, demonstrating the use of E-mail at an Infiniti dealership. In order to show how E-mail could be used to aid the management of the dealership, Eaton randomly selected a message sent by Bourke to an employee of the dealership. 'Unfortunately, Bourke's E-mail was of a personal, sexual, nature and not business-related.

4) Eaton reported this incident to her supervisor, who with management's authorization reviewed the E-mail messages of the entire work group. Nissan found substantial numbers of personal, including sexual, messages from Bourke and Hall, and issued written warnings to plaintiffs for violating the company policy prohibiting the use of the company computer system for personal purposes.

5) Over the course of her employment with Nissan, Bourke received periodic written performance reviews which indicated that she had problems in the areas of decision making, oral communication skills, job knowledge, and working with her peers. In her annual performance review, which she received in October 1990, Bourke was rated as "needs improvement," the second lowest of six levels.

6) When Hall's performance was reviewed on an interim basis in May 1990, she received an overall borderline satisfactory rating. Her performance was rated unsatisfactory in certain areas. She was criticized for spending to much time on personal business, and was told that she needed to demonstrate greater initiative and to put forth a greater effort to learn the computer system. In her annual performance review, Hall's overall evaluation was unsatisfactory, the lowest of six possible ratings. Her job performance deteriorated after the October 1990 review.

7) On December 28, 1990, while Nissan was closed for the Christmas holiday, plaintiffs filed grievances with Nissan's human resources department, complaining that the company had invaded their privacy by retrieving and reading their E-mail messages.

8) On January 2, 1991, Bourke was given a final warning notice, which stated that her performance would be monitored over the next three months and that she would be terminated if she did not meet the performance objectives outlined in the notice. Bourke resigned her position the next day. On that same day, Nissan terminated Hall. Hall had already accepted a job with another company, and was not surprised that she had been fired.

9) Based upon Nissan’s actions in reviewing their E-mail messages as described above, plaintiffs sued Nissan for common law invasion of privacy, violation of their constitutional right to privacy, and violation of the criminal wiretapping and eavesdropping statutes. They also stated a cause of action for wrongful discharge in violation of public policy, that is, termination in retaliation for the filing of complaints objecting to Nissan's invasion of their privacy.

10) Nissan moved for summary judgment, contending that there existed no disputed issue of material fact to warrant trial of the matter. The trial court found in Nissan's favor on two grounds: (1) Based on the undisputed facts, plaintiffs had no reasonable expectation of privacy in their E-mail messages; and (2) plaintiffs failed to submit a separate statement meeting the requirements of Code of Civil Procedure section 437c, subdivision (a) [FN1] and Law and Discovery Policy Manual Paragraph 207.

FN1. While the court and the parties all cite subdivision (a) of section 437c of the Code of Civil Procedure as the pertinent statutory provision, it is subdivision (b) of that section that prescribes the format and content of the separate statement required in support of and opposition to a summary judgment motion.

STANDARD OF REVIEW

11) Summary judgment is appropriate where the record establishes as a matter of law that no material disputed issue of fact exists or that the cause of action cannot prevail. (Wilkerson v. Wells Fargo Bank (1989) 212 Cal.App.3d 1217, 1224.) Because the motion raises only questions of law regarding the construction and effect of the supporting and opposing papers, this court will make its own independent determination of the questions of law raised in the motion. (Slivinsky v. Watkins-Johnson Co. (1990) 221 Cal.App.3d 799, 803-804; Wilkerson v Wells Fargo Bank, supra, at p. 1225.) In making this determination, the court will strictly construe the papers of the moving party, and resolve any doubts in favor of the party opposing the motion. (Isaacs v. Huntington Memorial Hospital (1985) 38 Cal.3d 112, 134-135.)

DISCUSSION

I

Common Law Invasion of Privacy and Violation of Constitutional Right to Privacy

12) Under the common law, "'[o]ne 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.' (Rest.2d, Torts § 652B.)" (5 Witkin, Summary of Cal. Law (9th ed. 1988) Torts, § 580, p. 674.) Moreover, Article 1, section 1 of the California Constitution establishes privacy as a fundamental right of citizens of this state. Because the constitutional right to privacy is broader than, and encompasses, the common law tort of invasion of privacy (see Porten v. University of San Francisco (1976) 64 Cal.App.3d 825, 829), we restrict our analysis to a discussion of the constitutional claim.

13) Whether an individual's constitutional right to privacy has been violated depends first on a determination whether that individual had a personal and objectively reasonable expectation of privacy which was infringed. (Alarcon v. Murphy (1988) 201 Cal.App.3d 1, 5; People ex rel. Franchise Tax Bd. v. Superior Court (1985) 164 Cal.App.3d 526, 540-541.) Nissan maintains that the evidence conclusively establishes that plaintiffs had no reasonable expectation of privacy in their E-mail messages. In support of this contention, they cite the following undisputed facts: (1) Plaintiffs each signed a Computer User Registration Form, which states that "[I]t is company policy that employees and contractors restrict their use of company-owned computer hardware and software to company business." (2) In November or December of 1989, more than a year before her termination, Hall learned from co-workers that E-mail messages were, from time to time, read by individuals other than the intended recipient. Hall relayed this information to Bourke in March of 1990. (3) In June 1990, a full six months before Bourke's termination, a fellow employee, Lori Eaton, contacted Bourke to complain about the personal, sexual nature of Bourke's E-mail message which Eaton had retrieved for demonstration purposes during a training session at an Infiniti dealership.

14) Nissan contends that the foregoing uncontroverted facts regarding plaintiffs knowledge that E-mail messages could in fact be read without the author's knowledge or consent establishes as a matter of law that plaintiffs had no objectively reasonable expectation of privacy in those messages. In contradiction of that conclusion, plaintiffs assert that they had such an expectation because they were given passwords to access the computer system and were told to safeguard their passwords. While plaintiffs' statements

that they believed that their E-mail messages would remain private may be sufficient, on a motion for summary judgment, to raise the issue of plaintiffs' subjective understanding, the question presented to us is whether their expectations of privacy were objectively reasonable as a matter of law. We agree with the trial court that they were not.

15) In the absence of a reasonable expectation of privacy, there can be no violation of the right to privacy. (Alarcon v. Murphy, supra, 201 Cal.App.3d 1, 5.) Thus, plaintiffs' causes of actions for common law invasion of privacy and violation of the constitutional right to privacy were properly dismissed on summary judgment.

II

Violation of Penal Code section 631

16) Penal Code section 631 prohibits a person from "intentionally tap[ping], or mak[ing] any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument, . . . or . . . read[ing], or attempt[ing] to read, or to learn the contents of any message, report, or communication while the same is in transit or passing over any wire, line or cable . . .." Penal Code section 637.2 provides a civil right of action against one who violates the wiretapping and eavesdropping statutes.

17) Plaintiffs have cited no authority to support their contention that section 631 covers the retrieval, printing and reading of E-mail messages which is not authorized by the author of the message. And by its express terms, the statute does not apply to the facts of this case: (1) There is no allegation that Nissan "tapped" into its own telephone lines, and indeed there would be no need to do so since, being the system operator, Nissan had access to the network without resort to a telephone line tap. (2) Likewise, as the owner and operator of the system, Nissan's connection to the telephone lines or cable which connected the system would necessarily be authorized. And (3) Nissan did not access the messages during transmission. Rather, the messages were retrieved from an electronic storage device and printed so that they could be read. Nissan's actions in retrieving, printing and reading plaintiffs' E-mail messages simply are not included within the actions proscribed by Penal Code section 631. While plaintiffs may argue that the law is outdated, judges are not authorized to amend statutes even to bring them up-to-date.

III

Violation of Penal Code Section 632

18) Penal Code section 632 prohibits the eavesdropping or recording of a "confidential communication by means of any electronic amplifying or recording device." Again, the plain words of the statute simple do not permit a finding that Nissan's conduct violated the law, as no amplifying or recording device was used to retrieve and read plaintiffs' E-mail messages. Moreover, the court of appeal has held that section 632 proscribes only "the interception of communications by the use of equipment which is not connected to any transmission line" (People v. Ratekin (1989) 212 Cal.App.3d 1165, 1168), a circumstance not present in this case.

IV

Wrongful Discharge in Violation of Public Policy

19) In the absence of an agreement to the contrary, an employee may be terminated at-will, that is, for any reason or for no reason at all. (Foley v. Interactive Data Corp. (1988) 47 Cal.3d 654, 665.) An employer may not, however, fire an employee for a reason which violates public policy, "since otherwise the threat of discharge could be used to coerce employees into committing crimes, concealing wrongdoing, or taking other action harmful to the public weal." (Ibid; see also, Tameny v. Atlantic Richfield (1980) 27 Cal.3d 167, 178 [employee terminated for refusing to engage in price-fixing]; Petermann v. International Brotherhood of Teamsters (1959) 174 Cal.App.2d 184, 188 [employee terminated for refusing to commit perjury].)

20) Plaintiffs contend that they were fired in retaliation for filing complaints about Nissan's review of their E-mail messages, and that their terminations therefore violated the public policy of the State of California that its citizen should be free from unauthorized and unreasonable intrusions into their private lives. A claim for wrongful termination in violation of public policy necessarily requires a violation of public policy. We concluded in Section I above that Nissan's actions in reviewing plaintiffs~ E-mail messages did not violate their constitutional right to privacy. Therefore, plaintiffs have failed to state a claim for wrongful termination in violation of public policy.

21) Because we conclude that plaintiffs' claims were properly disposed of on summary judgment since there were no disputed issues of material fact requiring a trial of the matter, we need not decide whether the trial court abused its discretion in dismissing the action for plaintiffs' failure to submit a separate statement of facts pursuant to Code of Civil Procedure section 437c, subdivision (b).

DISPOSITION

The judgment is affirmed.

NOT TO BE PUBLISHED

ARMSTRONG, J.

We concur:

TURNER, P.J.

GRIGNON, J.

Leventhal v. Knapek

UNITED STATES COURT OF APPEALS

FOR THE SECOND CIRCUIT

August Term, 2000

(Argued: April 19, 2001 Decided: September 26, 2001)

Docket No. 00-9306

GARY LEVENTHAL,
Plaintiff-Appellant,
v.
LAWRENCE KNAPEK, Individually and as Assistant Commissioner for the Office of Budget and Finance of the Department of Transportation of the State of New York, JOHN SAMANIUK, Individually and as Director of the Office of Internal Audit and Investigation of the Department of Transportation of the State of New York, LOUIS P. DESOL, Individually and as Director of the Employee Relations Bureau of the Department of Transportation of the State of New York, MICHAEL J. MCCARTHY, Individually and as the Director of the Division of Budget and Finance of the Department of Transportation of the State of New York, THERESA VOTTIS, Individually and as Associate Internal Auditor in the Office of Internal Audit and Investigation of the Department of Transportation of the State of New York, NEW YORK STATE DEPARTMENT OF TRANSPORTATION and JOSEPH H. BOARDMAN, Individually and as Commissioner of the Department of Transportation of the State of New York,

Defendants-Appellees.

Before: LEVAL, SACK, and SOTOMAYOR, Circuit Judges.

Appeal from a judgment of the United States District Court for the Northern District of New York (Norman A. Mordue, Judge) granting defendants' motion for summary judgment, denying plaintiff's cross-motion for summary judgment, and dismissing the complaint in a suit arising from defendants' search of plaintiff's workplace computer.

Even though, based on the particular facts of this case, plaintiff had some expectation of privacy in the contents of his computer, the searches were reasonable in light of the Department of Transportation's need to investigate allegations of misconduct as balanced against the modest intrusion caused by the searches. Plaintiff's constitutional due process rights were not violated by his loss of a provisional job appointment and failure to receive a discretionary salary increase because neither involved a property or liberty protected by the Fourteenth Amendment.

Affirmed.

BRIAN J. O'DONNELL, Rowley, Forrest, O'Donnell & Beaumont, P.C., Albany, New York (Jessica R. Wilcox on the brief), for plaintiff-appellant.

JULIE M. SHERIDAN, Assistant Solicitor General (Eliot Spitzer, Attorney General of the State of New York, Daniel Smirlock, Deputy Solicitor General, Peter H. Schiff, Senior Counsel), for defendants-appellees.
SOTOMAYOR, Circuit Judge:

After receiving anonymous allegations that an employee reasonably suspected to be plaintiff-appellant Gary Leventhal was neglecting his duties in the Accounting Bureau of the New York State Department of Transportation ("DOT"), DOT investigators, without Leventhal's consent, printed out a list of the file names found on Leventhal's office computer. The list of file names contained evidence that certain non-standard software was loaded on Leventhal's computer. This led to additional searches confirming that Leventhal had a personal tax preparation program on his office computer and to disciplinary charges against Leventhal for misconduct. After settling the disciplinary charges, Leventhal sued defendants-appellees, challenging the legality of the searches and of two employment actions taken against him.

We affirm the district court's grant of summary judgment to defendants, its denial of Leventhal's cross motion for summary judgment, and its dismissal of the complaint. Even though, based on the particular facts of this case, Leventhal had some expectation of privacy in the contents of his computer, the searches were reasonable in light of the DOT's need to investigate the allegations of Leventhal's misconduct as balanced against the modest intrusion caused by the searches. With respect to the challenged employment actions, Leventhal's constitutional due process rights were not violated by his loss of a provisional job appointment and his failure to receive a discretionary salary increase because neither involved property or liberty interests protected by the Fourteenth Amendment. Because we find that the DOT did not violate Leventhal's Fourth or Fourteenth Amendment rights, there is no need for us to address whether defendants enjoyed qualified immunity from suit.

BACKGROUND
Leventhal began his career at the DOT in 1974. At the time of the searches in question, Leventhal had risen to the position of Principal Accountant in the Accounting Bureau of the DOT, a grade 27 position. In 1996, and for several previous years, Leventhal maintained a private tax practice while employed at the DOT. He received DOT approval to make up on weekends or after normal work hours any time he missed because of his outside employment. In order to receive approval for this arrangement, Leventhal declared that his outside employment would "not interfere with the complete and proper execution of my duties with the Department of Transportation."

A. DOT Policies and Procedures

The DOT had a written policy prohibiting theft. The policy broadly defined theft to include:

improper use of State equipment, material or vehicles. Examples include but are not limited to: conducting personal business on State time; using State equipment, material or vehicles for personal business; improper use of the mail, copiers, fax machines, personal

computers, lincs codes or telephones and time spent on non-State business related activities during the workday.

During the DOT's interrogation of Leventhal after the searches of his office computer, Leventhal acknowledged that using DOT equipment for private purposes was "a violation of [DOT] policies."

The DOT also had an unwritten rule that only "standard" DOT software could be loaded on DOT computers. Although this rule was never officially promulgated as a DOT policy, Leventhal remarked during his interrogation that "the stated policy" was that employees were not to have personal software on a DOT computer "without permission." Nevertheless, it was known that the staff of the Accounting Bureau had loaded unlicensed copies of "non-standard" software on DOT computers and used the software to perform work-related activities due, at least in part, to the DOT's inability to purchase needed software for its employees. The DOT also had an official policy restricting office Internet access to DOT business.

In July 1996, the DOT circulated a memo from Ann Snow, the Network Administrator for the Budget and Finance Division, which stated that only original, licensed copies of software could be installed on DOT computers. Following the distribution of this memo, however, Leventhal's supervisors discussed their difficulties in complying with the memo because of the department's dependance upon the use of unlicensed software. Leventhal's immediate supervisor at the time, John Chevalier, instructed his subordinates, including Leventhal, that they could continue to use non-standard software for departmental business.

DOT computers were accessible, for certain limited purposes, by those other than their normal users. The computer support staff of the DOT engaged in troubleshooting and the upgrading of individual computers. During these maintenance operations, it was possible for the computer staff to observe whether non-standard DOT software had been loaded on an individual computer. DOT computers were also occasionally accessed without the user's knowledge to retrieve a needed document, sometimes bypassing a password prompt to obtain access. The computer staff of the DOT provided technical support for Leventhal's DOT computer upon his request three or four times between 1994 and 1996, and once, after hours, without his request, in order to change the name of the server.

B. The Anonymous Letter to the Inspector General

On October 15, 1996, the New York State Office of the Inspector General referred to the DOT an anonymous letter it had received complaining of abuses at the DOT Accounting Bureau. This letter described specific employees by reference to their salary grades, genders, and job titles, without providing names. The letter made certain allegations concerning a grade 27 employee. Leventhal was the only grade 27 employee in the office at that time and, therefore, the DOT investigators inferred that the grade 27 employee described in the letter was Leventhal. The relevant portion of the letter states:

The abuse of time and power is so far out of line with the intended functions of the bureau that to cite all specifics would be an endless task. The day to day operation of this bureau is a slap in the face to all good state workers. You have to see this place to believe it. I will cite a few examples. A grade 27 who is late everyday. The majority of his time is spent on non-DOT business related phone calls or talking to other personnel about

personal computers. He is only in the office half the time he is either sick or on vacation. . . . [Half the time of a grade 23] is spent playing computer games and talking on the phone to his family or talking sports to one his subordinates, the guy who sleeps at his desk. . . . A grade 18 with an apparent alcohol problem who is so incompetent that his supervisor allows him to sleep at his desk. The grade 27 is aware of this problem. When [the grade 18] is not sleeping he is playing computer games or drafting up letters which are typed by [another] grade 18, who is barely able to function at an entry level clerical position. . . . And the sad part is that management knows what is going on although they would deny it if you asked them . . . . I think its [sic] time for some new leadership in the bureau.

C. The DOT Searches

Lawrence Knapek, the Assistant Commissioner of the DOT for the Office of Budget and Finance, met with John Samaniuk, the acting director of the Office of Internal Audit and Investigations, and Gary Cuyler, the chief investigator for that office, to discuss how to respond to the allegations made in the letter. They decided that the Office of Internal Audit and Investigation would conduct an investigation employing "such techniques as reviewing telephone records, reviewing computer records, Internet logs, that kind of thing." A "computer review" was ordered for all of the employees who could be identified from the letter. This involved printing out a list of file names found on these DOT computers to determine whether any contained non-standard software. After business hours on October 25, 1996, the investigators entered Leventhal's office through an open door, turned on his DOT computer, and reviewed the directories of files on the computer's hard drive. There was no power-on password to gain access to Leventhal's computer, but once the machine was turned on, some of the menu selections that appeared were password-protected. In order to perform their search, the investigators may have used a "boot-disk," a disk which allows the computer to start up without encountering the menus normally found there.

Having located the computer directories, the investigators printed out a list of the file names to enable the later identification of the programs loaded on Leventhal's computer without having to open each program. This included a printout of the names of the "hidden" files on Leventhal's computer. These "hidden" directories, the investigators found, contained "Morph," a type of drawing program and "PPU," a program suspected of containing tax software because of file names such as "TAX.FNT," and "CUSTTAX.DBF." On the non-"hidden" directories, the investigators found other non-standard software, including the programs Prodigy, Quicken, and Lotus Suite (although one part of Lotus Suite was standard DOT software at the time). Over the next two months, the investigators reviewed the computers of other management personnel of the Accounting Bureau, including the Accounting Bureau's director, John Chevalier, and three Grade 23 employees, Glenn Walker, John DeFrancesco, and Herbert Whitmarsh.

In February 1997, DOT management and investigators met to examine the results from these searches. Assistant DOT Commissioner Knapek attended the meeting and, aware of Leventhal's private tax practice, was particularly interested in confirming the investigators' suspicion that Leventhal had loaded tax software on his DOT office computer. They decided to conduct a further search of Leventhal's computer to determine with greater certainty whether the "PPU" directory they had discovered during the first search was part of a tax preparation program. Investigators reexamined the computer in Leventhal's office once in February 1997 and twice in April 1997. During these

subsequent searches, they copied the "Morph" and "PPU" directories onto a laptop computer, obtained additional printouts of the file directories, and opened a few files to examine their contents. In the first April search, an investigator noticed that some items had been added to the PPU directory since the previous search, indicating recent activity. The PPU directory was later identified as belonging to "Pencil Pushers," a tax preparation program.

On May 2, 1997, shortly after informing Leventhal that he was under investigation and that the computer in his office would be confiscated, the Director of the DOT Employee Relations Bureau observed Leventhal appearing to delete items from his computer directories. Leventhal was then interrogated. He admitted to belonging to a group that had jointly purchased a single copy of the Pencil Pushers software that was then copied onto his computer and the computers of other members of the group. Leventhal also admitted that he had printed out up to five personal income tax returns from the computer in his DOT office.

D. The Disciplinary Proceeding Against Leventhal

In September 1997, the DOT brought disciplinary charges against Leventhal under N.Y. Civ. Serv. Law § 75 charging six grounds of misconduct or incompetence. 1 The DOT designated a private attorney as a hearing officer to take evidence and make recommendations to the Commissioner of the DOT, who would then review these recommendations and issue a decision in conformity with N.Y. Civ. Serv. Law § 75. The hearing officer began by holding a hearing concerning the admissibility of the evidence obtained during the DOT searches. On May 10, 1999, the hearing officer determined that the evidence acquired during the computer searches should be suppressed, finding that it had been obtained in violation of Leventhal's Fourth Amendment rights. The hearing officer notified the DOT Commissioner of his decision. In response, the Commissioner instructed the hearing officer to continue to take evidence, including all of the evidence obtained through the computer searches, and to forward to him the complete record, together with all of the hearing officer's recommendations. The hearing officer refused to comply with the request that he make the evidence from the searches part of the record. Three months later, on October 18, 1999, Leventhal settled with the DOT. As part of the settlement, the DOT agreed to withdraw all disciplinary charges except that of lateness, to which Leventhal pleaded guilty. As a result, Leventhal was penalized thirty work days leave without pay.

Between the time of the DOT searches of Leventhal's office computer and the time Leventhal was charged with misconduct, Leventhal was transferred from his position as Principal Accountant, a grade 27 position, to a position as the Supervisor of Agency Accounts, a grade 25 position. The DOT claims that this move was not precipitated by the disciplinary proceedings against Leventhal. Leventhal's 1994 promotion to his grade 27 position from a grade 25 position as Supervisor of Agency Accounts, was contingent on the ability of the person who had provisionally moved out of Leventhal's grade 27 position, John Chevalier, to retain the next highest position. Chevalier then failed to win permanent assignment to his higher-ranking position and, consequently, was moved back to the grade 27 position, forcing Leventhal back down to his former grade 25 position. Leventhal claims, however, that but for the disciplinary proceedings, the DOT would have created a special "663 position," akin to a grade 29 position, for Chevalier, allowing Leventhal to retain his grade 27 position.

In addition, on September 28, 1998, the DOT notified Leventhal that, due to the disciplinary charges pending against him, he would not be granted the 3.5% salary increase provided to most other management employees. At the option of the director of the budget, this salary increase could, by law, be withheld from any employee to reflect substandard job performance or when the increase was otherwise inappropriate. 1995 N.Y. Laws Ch. 314 § 3(11). Leventhal claims that he was denied this salary increase in retaliation for contesting the disciplinary charges against him.

E. Leventhal's Suit Against the DOT

Four days after he settled the DOT disciplinary charges, Leventhal filed this action in United States District Court for the Northern District of New York (Norman A. Mordue, Judge). In his complaint, Leventhal alleged, under 42 U.S.C. § 1983: (1) Fourth Amendment violations arising out of the computer searches; and (2) Fourteenth Amendment due process violations resulting from his demotion and the denial of the salary increase. 2

As a preliminary matter, the district court determined that the hearing officer's finding of a Fourth Amendment violation did not have preclusive effect on these proceedings. Regarding the propriety of the searches, the court found that Leventhal "could not reasonably expect complete privacy in the contents of his computer" because it was reasonable to expect "that other DOT employees might view the directory structure and other contents of his computer in his absence." Turning to the justification for the governmental intrusion, the district court concluded that the allegations in the anonymous letter were sufficient to give "rise to the reasonable suspicion that [Leventhal] was engaging in his private tax preparation business during work hours and that he might be using his computer in connection with that business" and that "an examination of the directory of the computer would produce evidence of work-related misconduct." On this basis, the court found that the scope of the initial search was reasonable and that the evidence discovered thereby justified the searches that followed. The district court rejected Leventhal's due process challenges to the DOT's failure to award him the 3.5% salary increase and his demotion to a grade 25 position, reasoning that Leventhal had no legal entitlement to either benefit.

DISCUSSION

A. Standard of Review

This Court reviews the grant of defendants' motion for summary judgment de novo, construing the evidence in the light most favorable to Leventhal as the non-moving party. See Tenenbaum v. Williams, 193 F.3d 581, 593 (2d Cir.1999), cert. denied, 529 U.S. 1098 (2000). Summary judgment is appropriate where "there is no genuine issue as to any material fact and . . . the moving party is entitled to a judgment as a matter of law," Fed. R. Civ. P. 56(c), and, therefore, "the record taken as a whole could not lead a rational trier of fact to find for the non-moving party." Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 587 (1986). A fact is "material" for these purposes if it "might affect the outcome of the suit under the governing law." Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986). An issue of fact is "genuine" if "the evidence is such that a reasonable jury could return a verdict for the nonmoving party." Id.

B. Leventhal's Fourth Amendment Claim

1. The Preclusive Effect of the Hearing Officer's Ruling

Absent specific statutory guidance from Congress, the preclusive effect of prior unreviewed state administrative determinations upon a subsequent suit in federal court is a matter of federal common law. See Univ. of Tenn. v. Elliott, 478 U.S. 788, 796-99 (1986) (fashioning common law rules for issue preclusion in suit under 42 U.S.C. § 1983). When federal common law gives preclusive effect in federal court to a state administrative determination, that prior determination has "the same preclusive effect to which it would be entitled in the State's courts." Id. at 799.

In this case, we need not reach the issue of whether federal common law would give preclusive effect to this state administrative determination because, even if it did, the action by the hearing officer would not have preclusive effect under New York law. 3 Under New York law, a state agency determination is given preclusive effect in a subsequent state court proceedings only when, inter alia, the identical issue, see Allied Chem. v. Niagara Mohawk Power Corp., 528 N.E.2d 153, 155 (N.Y. 1988), has "been decided in the prior action." Schwartz v. Public Adm'r of the Bronx, 246 N.E.2d 725, 729 (N.Y. 1969). In this case, the hearing officer's conclusion that Leventhal's Fourth Amendment rights were violated does not have preclusive effect because the issue was not "decided" in the agency proceeding. Leventhal and the DOT settled the disciplinary action before the hearing had concluded and the hearing officer's final recommendations had been forwarded to the DOT Commissioner for "review and decision." N.Y. Civ. Serv. Law § 75(2). Even if the hearing officer were to have completed taking the evidence and had offered recommendations, only the DOT Commissioner can make the agency determination. See Simpson v. Wolansky, 343 N.E.2d 274, 276 (N.Y. 1975) ("[T]he findings of the hearing officer [in a N.Y. Civ. Serv. Law § 75 proceeding] are not conclusive and may be overruled by the official upon whom has been imposed the power to remove or mete out the discipline."). Although Leventhal points to one case indicating that a hearing officer "receives and rules on evidence, keeps a record of the proceeding, and makes a recommendation to the disciplinary authority," Anderson v. Dolce, 653 F. Supp. 1556, 1563 (S.D.N.Y. 1987) (emphasis added), the same case notes that "[t]he disciplinary authority is not bound by the hearing officer's recommendation." Id. at 1563.

2. Public Employer Searches in Government Workplaces

"[T]he Fourth Amendment protects individuals from unreasonable searches conducted by the Government, even when the Government acts as an employer." Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665 (1989). The "special needs" of public employers may, however, allow them to dispense with the probable cause and warrant requirements when conducting workplace searches related to investigations of work-related misconduct. See O'Connor v. Ortega, 480 U.S. 709, 719-26 (1987) (plurality opinion); id. at 732 (Scalia, J. concurring). In these situations, the Fourth Amendment's protection against "unreasonable" searches is enforced by "a careful balancing of governmental and private interests." New Jersey v. T.L.O., 469 U.S. 325, 341 (1985) (discussing the reasonableness of a search in the absence of a warrant and probable cause). A public employer's search of an area in which an employee had a reasonable expectation of privacy is "reasonable" when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of" its purpose. O'Connor, 480 U.S. at 726 (plurality opinion) (internal quotation marks omitted).

We begin by inquiring whether "the conduct . . . at issue . . . infringed an expectation of privacy that society is prepared to consider reasonable." Id. at 715 (plurality opinion) (internal quotation marks omitted). Without a reasonable expectation of privacy, a workplace search by a public employer will not violate the Fourth Amendment, regardless of the search's nature and scope. The workplace conditions can be such that an employee's expectation of privacy in a certain area is diminished. See id. at 717-18 (plurality opinion) (recognizing that offices that are "continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits," can be "so open to fellow employees or the public that no expectation of privacy is reasonable."); id. at 737 (Blackman, J., dissenting) ("[I]n certain situations, the 'operational realities' of the workplace may remove some expectation of privacy on the part of the employee."). On the facts of O'Connor, the entire Court found a reasonable expectation of privacy with respect to the office desk and file cabinets in which the plaintiff had maintained his personal correspondence, medical files, correspondence from private patients unconnected with his employment, personal financial records, teaching aids and notes, and personal gifts and mementos. Id. at 718 (plurality opinion); id. at 731 (Scalia, J., concurring); id. at 732 (Blackmun, J., dissenting). In finding that the plaintiff had a reasonable expectation of privacy, the plurality noted that there was no evidence that the employer had "established a[ ] reasonable regulation or policy discouraging employees . . . from storing personal papers and effects in their desks or file cabinets." Id. at 719 (plurality opinion).

3. Leventhal's Expectation of Privacy

We hold, based on the particular facts of this case, that Leventhal had a reasonable expectation of privacy in the contents of his office computer. We make this assessment "in the context of the employment relation," id. at 717 (plurality opinion), after considering what access other employees or the public had to Leventhal's office.

Leventhal occupied a private office with a door. He had exclusive use of the desk, filing cabinet, and computer in his office. Leventhal 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.

We are aware that "[p]ublic employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." Id. Construing the evidence in favor of Leventhal, as we must in reviewing this grant of summary judgment against him, we do not find that the DOT either had a general practice of routinely conducting searches of office computers or had placed Leventhal on notice that he should have no expectation of privacy in the contents of his office computer. Cf. United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (finding no legitimate expectation of privacy in Internet use when employer's known policy allowed monitoring of "all file transfers, all websites visited, and all e-mail messages"); Sheppard v. Beerman, 18 F.3d 147, 152 (2d Cir. 1994) (finding no legitimate expectation of privacy in office, desk, and file cabinets in light of the "unique" relationship between a judge and her law clerk necessitating a "distinctive open access to documents").

Viewing the DOT anti-theft policy in the light most favorable to Leventhal, we find that it did not prohibit the mere storage of personal materials in his office computer. Rather, the anti-theft policy prohibited "using" state equipment "for personal business" without

defining further these terms. John Samaniuk, acting director of the DOT's Office of Internal Audits and Investigations, testified at Leventhal's disciplinary hearing that an employee would not violate state policies by keeping a personal checkbook in an office drawer, even though it would take up space there. Under the circumstances presented here, we cannot say that the same anti-theft policy prohibited Leventhal from storing personal items in his office computer. See O'Connor, 480 U.S. at 719 (plurality opinion) (finding "a reasonable expectation of privacy at least in [an office] desk and file cabinets").

Although the DOT technical support staff had access to all computers in the DOT offices, their maintenance of these computers was normally announced and the one example in the record of an unannounced visit to Leventhal's computer was only to change the name of a server. DOT personnel might also need, at times, to search for a document in an unattended computer, but there was no evidence that these searches were frequent, widespread, or extensive enough to constitute an atmosphere "so open to fellow employees or the public that no expectation of privacy is reasonable." Id. at 718 (plurality opinion). This type of infrequent and selective search for maintenance purposes or to retrieve a needed document, justified by reference to the "special needs" of employers to pursue legitimate work-related objectives, does not destroy any underlying expectation of privacy that an employee could otherwise possess in the contents of an office computer. The Supreme Court has concluded that "'[c]onstitutional protection against unreasonable searches by the government does not disappear merely because the government has the right to make reasonable intrusions in its capacity as employer.'" Id. at 717-18 (plurality opinion quoting concurring opinion of Scalia, J) (emphasis in original). 4

4. The Nature and Scope of the Searches

Even though Leventhal had some expectation of privacy in the contents of his office computer, the investigatory searches by the DOT did not violate his Fourth Amendment rights. An investigatory search for evidence of suspected work-related employee misfeasance will be constitutionally "reasonable" if it is "justified at its inception" and of appropriate scope. Id. at 726 (plurality opinion); see also T.L.O. 469 U.S. at 342 (finding search permissible in its scope when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct]"). We agree with the district court that both of these requirements are satisfied here.

The initial consideration of the search's justification examines whether "there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct." O'Connor, 480 U.S. at 726 (plurality opinion). Here, there were reasonable grounds to believe that the searches would uncover evidence of misconduct. The specific allegations against the grade 27 employee, who was reasonably assumed to be Leventhal, were that (1) he was "late everyday"; (2) he spent "[t]he majority of his time . . . on non-DOT business related phone calls or talking to other personnel about personal computers"; and that (3) "[h]e is only in the office half the time[; the other half] he is either sick or on vacation." Probable cause is not necessary to conduct a search in this context, a plurality of the Court has explained, because "public employers have a direct and overriding interest in ensuring that the work of the agency is conducted in a proper and efficient manner." Id. at 724 (plurality opinion). The individualized suspicion of misconduct in this case justified the DOT's decision to instigate some type of search. 5

The scope of a search will be appropriate if "reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct." Id. at 726 (plurality opinion) (alterations omitted). We conclude that the DOT search to identify whether Leventhal was using non-standard DOT software was "reasonably related" to the DOT's investigation of the allegations of Leventhal's workplace misconduct. Although the anonymous letter did not allege that the grade 27 employee was misusing DOT office computers, it did allege that the grade 27 employee was not attentive to his duties and spent a significant amount of work time discussing personal computers with other employees. Furthermore, the letter's allegations assumed that the DOT prohibition against misusing office computers was not rigorously enforced in the Accounting Bureau, remarking that a grade 18 employee "play[ed] computer games," that a grade 23 employee spent a substantial part of the day "playing computer games" or in non-work related conversations, and that another grade 23 employee "amuses himself by learning about computer software which have nothing to do with work." In view of the allegations of the misuse of DOT computers among other employees in the Accounting Bureau, Leventhal's alleged penchant for discussing personal computers during work hours, and Leventhal's general inattention to his duties which included, we presume, supervision of the computer use of others, we find that the searches of his computer were "reasonably related" to the DOT investigation of allegations of Leventhal's workplace misconduct.

Leventhal argues that a search for non-standard software would be irrelevant to charges of misconduct because the DOT had, de facto, approved of the use of non-standard software needed to conduct DOT business. Even assuming that this were true, the investigation was more broadly aimed at uncovering evidence that Leventhal was using his office computer for non-DOT purposes. The searches accomplished this task by uncovering evidence that Leventhal had loaded a tax preparation program onto his office computer, a program that he later admitted he used to print out personal tax returns in his office.

We also find that the scope of the searches was not "excessively intrusive in light of the nature of the misconduct." Id. at 726 (plurality opinion) (internal quotation marks and ellipsis omitted). During the first search, the DOT investigators printed out a list of file names found on Leventhal's office computer. They did not run any program or open any files. The investigators entered Leventhal's office through an open door and found that Leventhal's computer had no power-on password although some menu selections were password protected. The investigators limited their search to viewing and printing file names that were reasonably related to the DOT's need to know whether Leventhal was misusing his office computer. The first search was permissible in scope.

Neither were the three subsequent searches "excessively intrusive." After the first search had established that files named "TAX.FNT" and "CUSTTAX.DBF" were loaded on Leventhal's computer, the investigators reasonably suspected that these files were part of a tax program. When DOT investigators and management met to discuss what they had found in the first search, Assistant Commissioner Knapek expressed a particular interest in confirming whether Leventhal had loaded tax preparation software on his DOT computer, aware that Leventhal had a private tax practice. Investigators reexamined the computer in Leventhal's office once in February 1997 and twice in April 1997. These searches were limited to copying onto a laptop computer the "PPU" directories that they later identified as referring to "Pencil Pushers," a tax preparation program, and the "Morph" directories, pertaining to a graphics program, to printing out additional copies of

the file names, and to opening a few files to examine their contents. There is no evidence that the DOT opened and examined any computer files containing individual tax returns that may have been saved on Leventhal's computer, and, therefore, we need not address the permissibility of searching such materials. Considering that the first search yielded evidence upon which it was reasonable to suspect that a more thorough search would turn up additional proof that Leventhal had misused his DOT office computer, the DOT investigators were justified in returning to confirm the nature of the non-standard DOT programs loaded on Leventhal's computer by copying directories, printing file names, and opening selected files. 6

C. Leventhal's Due Process Claim

Leventhal claims that when the DOT demoted him and failed to award him a salary increase, it did so without the due process guaranteed to him by the Fourteenth Amendment. This claim fails because Leventhal did not possess a property or liberty interest protected by the Due Process Clause in either his former job grade or the salary increase.

In order to be protected by the Constitution against the deprivation of a government benefit without due process of law, a claimant must have a "legitimate claim of entitlement to it." Bd. of Regents of State Colleges v. Roth, 408 U.S. 564, 577 (1972). The expectation of entitlement is typically derived from "existing rules or understandings that stem from an independent source such as state law-rules or understandings that secure certain benefits." Id.; see also Bernheim v. Litt, 79 F.3d 318, 322 (2d Cir. 1996) ("To state a cause of action under the [D]ue [P]rocess [C]lause, a plaintiff must show that she has a property interest, created by state law, in the employment or the benefit that was removed.").

1. Salary Increase

Leventhal's discretionary salary increase was not a form of property protected by the Constitution against deprivation without due process of law. On September 28, 1998, the DOT notified Leventhal that, because of the pending disciplinary charges against him, he would not receive the 3.5% salary increase granted to most other management employees. The salary increase could, by law, be withheld from any employee who, in the opinion of the director of the budget, had substandard job performance or when the increase was otherwise unwarranted. 1995 N.Y. Laws Ch. 314 § 3(11). 7

Because Leventhal cannot satisfy the threshold requirement that the salary increase was his "property," the claim that he was deprived of the increase without due process of law must fail. See Bernheim, 79 F.3d at 323 ("[W]here the complained-of conduct concerns matters that are within an official's discretion, entitlement to that benefit arises only when the discretion is so restricted as to virtually assure conferral of the benefit.").

2. Demotion From Grade 27 to Grade 25

Similarly, Leventhal's demotion from a grade 27 to a grade 25 position was not offensive to the Due Process Clause of the Fourteenth Amendment. Leventhal concedes that his former grade 27 position as Principal Accountant was a "contingent permanent" position whose security depended upon John Chevalier, the person who had formerly occupied this position, being hired permanently at the grade 29 position of Director of

Transportation Accounting and Fiscal Services. Leventhal was moved back to his former grade 25 position after Chevalier retreated to his former position as Principal Accountant.

Leventhal argues that the DOT could have kept both him and Chevalier at their former pay grades if the DOT had created a special "663" position - equivalent to a grade 29 position - for Chevalier after Chevalier failed to win appointment as permanent chief of the Accounting Section. This argument suffers from the same infirmity already discussed. Even assuming that Leventhal had standing to challenge the DOT's failure to create a job for Chevalier, the DOT has not conferred on someone in Chevalier's situation a right to having a special "663" position created whenever that employee fails to win the permanent placement desired. As a result, the DOT's failure to create such a position in this case did not deprive Chevalier and, consequently, Leventhal, of any property interest protected by the Due Process Clause.

Additionally, Leventhal implies that his constitutional liberty interest was harmed because his demotion "'impose[d] on him a stigma or other disability that foreclose[s] his freedom to take advantage of other employment opportunities or that might seriously damage his standing and associations in his community.'" Brief of Plaintiff at 37 (quoting Roth, 408 U.S. at 573). On appeal, however, Leventhal has not specified anything within the allegedly stigmatizing material that is arguably false. This omission proves fatal to his claim. See Quinn v. Syracuse Model Neighborhood Corp., 613 F.2d 438, 446 (2d Cir. 1980) ("[T]o constitute deprivation of a liberty interest, the stigmatizing information must be both false and made public by the offending governmental entity.") (internal quotation marks and ellipses omitted).

CONCLUSION

Because the DOT searches of Leventhal's office computer were not "unreasonable" under the Fourth Amendment, and the DOT's demotion of Leventhal and its failure to grant him a salary increase were not deprivations of property or liberty warranting constitutional protection under the Fourteenth Amendment, we affirm the district court's grant of summary judgment to defendants, denial of Leventhal's cross-motion for summary judgment, and dismissal of the complaint. 8

---- Begin End Notes ----

1 The grounds were (1) lateness; (2) improper use of an office computer by installing non-standard personal software programs in violation of the DOT anti-theft policy; (3) improper business relationships between a subordinate and his superior in purchasing and sharing the cost of the Pencil Pushers software in violation of the DOT's conflict of interest policy; (4) improper use of DOT computer equipment in printing tax returns of private clients in violation of the DOT anti-theft policy; (5) interference with the DOT disciplinary investigation by deleting computer files from an office computer after being informed that the computer would be confiscated; and (6) violation of copyright infringement laws by the unlicensed installation and maintenance of the Pencil Pushers software on a DOT office computer subjecting the DOT to potential liability for copyright infringement.

2 By his failure to pursue them on appeal, we find that Leventhal has waived other claims made in his complaint. These include claims made under (1) the First Amendment; (2) the Equal Protection Clause of the Fourteenth Amendment; (3) the Fifth Amendment; (4) 42 U.S.C. § 1985; and (5) N.Y. Civ. Serv. Law § 75, independent of the Fourth Amendment search and seizure and Fourteenth Amendment due process brought under 42 U.S.C. § 1983 and discussed in this opinion. Leventhal has not challenged on appeal and, therefore, we conclude has abandoned any opposition to the district court's decision to bar, under the Eleventh Amendment, any claims for monetary damages against the DOT and individual defendants sued in their official capacity.

3 In Elliott, the Supreme Court found that preclusion applies in federal court "when a state agency acting in a judicial capacity resolves disputed issues of fact properly before it which the parties have had an adequate opportunity to litigate." Elliott, 478 U.S. at 789 (internal quotation marks and ellipsis omitted and emphasis added). Neither the Supreme Court nor this Court has decided whether preclusion would similarly apply in a suit under 42 U.S.C. § 1983 for an issue of law or a mixed question of law and fact resolved by the state agency such as those involved in the suppression of evidence under the Fourth Amendment. See Doe v. Pfrommer, 148 F.3d 73, 80 (2d Cir.1998) ("Currently, this circuit has not taken a position regarding the split in the circuits as to whether to give preclusive effect to the unreviewed legal determinations of state administrative decisions."). For purposes of this discussion we will assume, without deciding, that preclusion could apply under these circumstances to the unreviewed decision of a state administrative agency to exclude evidence it believed was obtained in violation of the Fourth Amendment.

4 Despite the split in the O'Connor court on other matters, there appears to be unanimity surrounding this principle. Justice Scalia, concurring in the judgment, would have gone further to declare that "the offices of government employees . . . are covered by Fourth Amendment protections as a general matter" except in unusual situations such as when "the office is subject to unrestricted public access." Id. at 731. The plurality opinion recognized that the presumption of workplace privacy could be defeated not only by public access by also when offices are "so open to fellow employees . . . that no expectation of privacy is reasonable." Id. at 718. Nevertheless, the plurality opinion quoted Justice Scalia's concurrence approvingly in stating that searches justified by an employer's special needs do not extinguish the underlying expectation of privacy. Id. at 717. The four dissenting justices similarly quoted with approval Justice Scalia's formulation. Id. at 738.

5 We do not reach the issue of whether a search would have been justified in the absence of individualized suspicion. See O'Connor, 480 U.S. at 726 ("Because petitioners had an 'individualized suspicion' of misconduct by [the plaintiff], we need not decide whether individualized suspicion is an essential element of the standard of reasonableness that we adopt today.").

6 On appeal, Leventhal has not pressed a claim that his constitutional rights were violated by the DOT seizure of his office computer and its contents on May 2, 1997. Accordingly, we find that any such claim has been abandoned.

7 The enactment provided, in relevant part, that:

[A]ny increase in compensation provided by this section . . . may be withheld in whole or in part from any officer or employee when in the opinion of the director of the budget, such withholding is necessary to reflect the job performance of such officer or employee, or to maintain appropriate salary relationships among officers of employees of the state, or to reduce state expenditures to acceptable levels or, when in the opinion of the director of the budget, such increase is not warranted or is not appropriate and the salary of such officer or employee is set at the discretion of the appointing authority.

1995 N.Y. Laws Ch. 314 § 3(11).

8 Accordingly, we also deny Leventhal's request under 42 U.S.C. § 1988 for attorneys' fees.

Pacific Northwest Herb Corp. v. Thompson

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

THE PACIFIC NORTHWEST HERB CORPORATION

PLAINTIFF

AND:

JAMES THOMPSON, also known as JIM THOMPSON

DEFENDANT

REASONS FOR JUDGMENT

OF THE

HONOURABLE MR. JUSTICE MELVIN

R. D. Holmes
Counsel for the Plaintiff

D. R. Eyford
Counsel for the Defendant

Place and Dates of Hearing:
Vancouver, British Columbia

October 14 & 28, 1999

[1] The defendant was employed as president of the plaintiff corporation and during the course of his employment, he utilized a computer owned by the plaintiff for business purposes and some personal activity. The defendant took the computer to his home at which time it was accessed not only by himself but also by other members of his family for personal reasons. The defendant's use in the main was for business in relation to his employment as president of the plaintiff corporation. A dispute having arisen between the plaintiff and the defendant, the plaintiff terminated the defendant's employment and commenced these proceedings alleging a number of items of inappropriate conduct on the part of the defendant while employed as president.

[2] After his dispute with the plaintiff, the defendant consulted solicitors concerning the plaintiff's claim and his counterclaim for wrongful dismissal. This consultation resulted

in correspondence by the defendant to his solicitors, which was prepared using the plaintiff's computer at the defendant's residence. In addition, the defendant was involved in matrimonial proceedings during the relevant period and corresponded with other solicitors whom he retained for those proceedings. This correspondence prepared and sent by the defendant to his solicitors was created by use of the plaintiff's computer that the defendant had at his home at all material times.

[3] The defendant "saved" the correspondence on the computer's hard drive. He could have "saved" the correspondence on disk but chose not to follow that course.

[4] Subsequently, during the course of this litigation, the defendant agreed to return the computer to the plaintiff. To facilitate its return while "protecting his correspondence to his solicitors" the defendant took the computer to a computer company, 3 Log Systems Incorporated. According to the affidavit of the president of that company, the defendant asked for his advice in assistance to erase data from the computer hard drive. As a result, Mr. Farzadeh recommended a procedure, which is, in his understanding, a common procedure to permanently erase files from a computer. The function performed according to the deponent destroys files but does not do any damage to the computer's hard drive.

[5] This process was confirmed by the defendant in his affidavit sworn the 14th day of May 1999 where he deposes that he "executed the command F-disk" to delete all of the documents and software on the computer.

[6] The effect of this process on the integrity of the computer is disputed. Mr. Atkinson, an officer of the plaintiff corporation, sought professional advice concerning the condition of the computer and was advised that a person knowledgeable enough to know the effect of the erasing process as carried out by the defendant, or an individual on his behalf, would also have known that the process would destroy the operating system of the computer.

[7] The integrity of the computer is not at issue in these proceedings save and except that the plaintiff, once the computer had been returned by the defendant, took steps to examine the contents of the computer as it had no knowledge of the defendant's use of the computer for purposes of corresponding with his solicitors.

[8] On receipt of the computer, the plaintiff reviewed its operations to determine what business records were contained within it. This was important to the plaintiff's claim as in part it relates to allegations that the defendant fraudulently charged expenses to the plaintiff. There is evidence to indicate that the defendant used the computer for business purposes including preparation of records, which were used to substantiate claims for expenses. While searching through the computer, one letter appeared which apparently was directed by the defendant to one of his solicitors. The opening wording is somewhat indecipherable. However, the plaintiff's officer, on identifying the nature of the letter, ceased reading it and reported the existence of the letter, not its contents, to its counsel who in turn advised the defendant's counsel of what occurred. The defendant apparently expected that the steps he took before returning the computer would safeguard his correspondence with his solicitors.

[9] As of this moment, the plaintiff has ceased accessing the computer for information or records relating to its business activities until the status of the defendant's solicitors' correspondence is resolved.

[10] It is in this context that the defendant seeks, pursuant to his notice of motion issued May 14, 1999, the following items of relief:

1. An order that the plaintiff deliver to the defendant a list of all the documents the plaintiff may have retrieved from the computer;
2. The plaintiff deliver to the defendant all documents and copies that have been made of documents that have been retrieved from the computer;
3. That the plaintiff and its servants or agents be enjoined from retrieving, creating or copying documents created by the defendant;
4. The plaintiff, and those having any knowledge of any order made in these proceedings, keep confidential the contents of the documents retrieved from the computer;
5. The representatives of the plaintiff who have knowledge of the documents retrieved be enjoined from instructing the plaintiff's solicitors in the conduct of the litigation.

[11] In the material filed by the plaintiff, it is alleged that the defendant did not have the plaintiff's authority to take the computer to his home or to use it for personal purposes. In my opinion, it is not necessary to resolve that dispute at this stage of the proceedings. It should be noted, however, that the defendant was at all times material the president of the plaintiff's company. Presumably self-authorization would be sufficient under the circumstances.

[12] It was suggested in the material filed that the defendant deliberately and intentionally damaged the computer prior to its return to the plaintiff. The conflicting passages in the respective affidavits have been set out above. Again, it is not necessary at this stage to resolve the impact of the defendant's actions on the usefulness of the computer. Suffice it to say that the defendant intended to remove his solicitors' correspondence and all of the software and the documents (see paragraph 18 of the defendant's affidavit, "to delete all of the documents and software on the computer --").

[13] Obviously the defendant's intentions were to deny the plaintiff access to the documents and to deny the plaintiff use of the software. In this respect, the defendant's conduct went beyond deletion of his solicitors' correspondence. His conduct deleted the plaintiff's business records. In response, the defendant asserts in his affidavit that the business records of the plaintiff, which were in the computer in question, were placed on a separate disk and returned to the plaintiff.

[14] A number of issues have arisen:

1. Are the documents prepared by the defendant and saved on the plaintiff's computer and sent to the defendant's solicitors subject to a right of confidentiality (privilege claim)?
2. Has any right of confidentiality (privilege claim) been lost or waived by the defendant returning the computer to the plaintiff?
3. Can or should the court restrain the plaintiff from accessing its computer and retrieving the defendant's correspondence to his solicitors?
4. Can or should the court restrain the plaintiff from accessing its computer and retrieving its business records?
5. Can or should the court restrain the plaintiff or its representatives who have the knowledge of the privileged documents from using the same.
6. Can or should the court restrain the plaintiff or its representatives from accessing documents prepared by the defendant or members of his family, which may be considered "confidential or private" documents.

SOLICITOR-CLIENT CONFIDENTIALITY (PRIVILEGE CLAIM)
[15] In Descoteaux et al v. Mierzwinski and Attorney General of Quebec et al (1982), 141 D.L.R. (3d) 590, the court discussed the nature of solicitor-client privilege in the following language at p. 601:

There is no denying that a person has a right to communicate with a legal adviser in all confidence, a right that it "founded upon the unique relationship of solicitor and client" (Solosky, ((1979), 50 C.C.C. (2d) 495; 105 D.L.R. (3d) 745; [1980] 1 S.C.R. 821) ...). It is a personal and extra-patrimonial right which follows a citizen throughout his dealings with others. Like other personal, extra-patrimonial rights, it gives rise to preventive and curative remedies provided for by law, depending on the nature of the agression (sic) threatening it or of which it was the object. Thus a lawyer who communicates a confidential communication to others without his client's authorization could be sued by his client for damages; or a third party who had accidentally seen the contents of a lawyer's file could be prohibited by injunction from disclosing them.
And further at p. 603:

The substantive rule
Although the right to confidentiality first took the form of a rule of evidence, it is now recognized as having a much broader scope, as can be seen from the manner in which this court dealt with the issues raised in Solosky, ...
Further at pp. 604 and 605:

It would, I think be useful for us to format the substantive rule, as the judges formerly did with the rule of evidence; it could, in my view, be stated as follows:
1. The confidentiality of communications between solicitor and client may be raised in any circumstances where such communications are likely to be disclosed without the client's consent.
2. Unless the law provides otherwise, when and to the extent that the legitimate exercise of a right would interfere with another person's right to have his communications with his lawyer kept confidential, the resulting conflict should be resolved in favour of protecting the confidentiality.
3. When the law gives someone the authority to do something which, in the circumstances of the case, might interfere with that confidentiality, the decision to do so and the choice of means of exercising that authority should be determined with a view to not interfering with it except to the extent absolutely necessary in order to achieve the ends sought by the enabling legislation.
[16] Prima facie the documents created by the defendant for his solicitors with reference to the current litigation or any possible matrimonial litigation are confidential. I should note, as to the content of any such communication, the documents themselves have not been produced to the court for inspection, a process which may be followed to resolve the issue of privilege claimed in the context of introduction of evidence. As to the identification of the correspondence, although the defendant has no particular means of recalling the dates or places or subjects of the correspondence, it is clear that insofar as they were sent to his solicitors, those solicitors should be in a position to identify by date and subject matter any correspondence which they received from the defendant.

[17] In Descoteaux, the court made it very clear that any dispute as to the confidentiality of documents should be resolved by supporting the confidentiality, and any interference with that confidentiality should be limited to what is absolutely necessary.

[18] The question then arises as to whether or not the defendant has waived a claim of privilege over the solicitors' correspondence. This issue was considered by the court in Fording Coal v. United Steel Workers of America, Local Union No. 7884 [1998] B.C.J. No. 1418, Vancouver Registry No. C982223. In Fording Coal, Lysyk J. followed the substantive rule in Descoteaux and then dealt with the issue of inadvertent waiver. In that context, he referred to Somerville Belkin Industries Ltd. v. Brocklesby Transport (1985), 65 B.C.L.R . 260 (S.C.) and Otting v. Elkford (District) (1992), 70 B.C.L.R. (2d) 202 (S.C.) and Tilley v. Hails (1993), 12 O.R. (3d) 306 (Ont. Gen. Div.) and concluded after a consideration of those authorities that privilege may be waived in civil cases only by the client and then only when it is waived deliberately and knowingly and not inadvertently. As Chapnik J. stated in Tilley v. Hails:

... where such communications are disclosed either inadvertently or through improper conduct by a party, that party's solicitors are not entitled to make use of the documents in the litigation: ...

[19] Consequently, inadvertent waiver does not suffice to destroy the privileged nature of communications between solicitor and client. In the case at bar, the issue is whether the defendant's conduct in returning the computer with correspondence on the hard drive constitutes a waiver of privilege claimed when the existence of that correspondence on the hard drive is unknown to the defendant. In this context, there is no doubt that the defendant acted deliberately in his attempts to remove the correspondence and there is no doubt that he believed that he succeeded. In addition, there is no doubt that the computer and its hard drive belong to and are the property of the plaintiff. The defendant's removal attempts are recognition by him of his expectation that the plaintiff would use its computer and retrieve what information remained. Under these circumstances, can it be said that the defendant waived any claimed privilege?

[20] Counsel for the plaintiff relies on Fording Coal where McLachlin J. in S & K Processors Ltd. v. Campbell Ave. Herring Ltd. (1983), 45 B.C.L.R. 218 (S.C.) discussed two types of waiver at p. 220:

Waiver of privilege is ordinarily established where it is shown that the possessor of the privilege: (1) knows of the existence of the privilege; and (2) voluntarily evinces an intention to waive that privilege. However, waiver may also occur in the absence of an intention to waive, where fairness and consistency so require. Thus waiver of privilege as to part of a communication will be held to be waiver as to the entire communication. Similarly, where a litigant relies on legal advice as an element of a claim or defence, the privilege which would otherwise attach to that advice is lost Rogers v. Hunter, [1982] 2 W.W.R. 189, 34 B.C.L.R. 206 (S.C.).

[21] In this respect, counsel relies on the fairness and consistency basis for conclusion that absence of an intention waiver may also occur. This submission is based on the recognition that the defendant is the author of his own misfortune as his conduct has created the difficulty that now exists. Counsel for the plaintiff submits that the whole problem could have been avoided if:

(a) the defendant did not use the plaintiff's computer;
(b) the defendant did not save the correspondence on the hard drive;
(c) the defendant communicated with his solicitors before the computer was returned to the plaintiff.

[22] No doubt each of these statements is correct. The defendant's conduct in deleting all documents and the software is subject to significant criticism as his attempt to delete his

solicitors' correspondence, adversely, even if temporarily, affects the plaintiff's ability to use its own equipment.

[23] That does not, in my opinion, justify a conclusion that the defendant has waived the privilege he claims associated with solicitor-client correspondence. The disclosure to the plaintiff of the existence of the content of otherwise privileged correspondence, in my opinion, was inadvertent. Consequently, I am satisfied the defendant's conduct did not amount to waiver of the privilege within the meaning of the authorities.

PRIVATE OR PERSONAL DOCUMENTS

[24] In this respect, it is submitted on behalf of the defendant that certain documents created by the defendant by using the plaintiff's computer and presumably "saved" on the hard drive of the plaintiff's computer are private or confidential. The documentation referred to may be described as family correspondence, children's correspondence, school assignments and matters which pertain to the family life of the defendant and are not associated in any way, shape or form with his past employment with the plaintiff. In this respect, counsel for the defendant submits that there is a right of privacy as recognized by s. 1 of the Privacy Act, R.S.B.C. 1996, c. 373 which states:

(1) It is a tort, actionable without proof of damage, for a person, wilfully and without claim of right, to violate the privacy of another.
(2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.
(3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.
[25] In R. v. Stewart (1988), 44 C.C.C. (3d) 481, the court referred to an article in (1988), 38 U.T.L.J. 117 by Professor Weinrib and noted that a submission could be made that confidential information is property for the purposes of civil law and that the cases demonstrate that Canadian and English civil law protect confidential information without clearly establishing a legal basis to do so. The Supreme Court of Canada notes that as of that date, no Canadian authority had so far conclusively decided that "confidential information is property".

[26] Accepting that the defendant may have a reasonable expectation of privacy, in relation to documents which he has created for his own personal use or for his family use and that such documents have a "confidential" component in that respect for purposes only of these reasons, it is then necessary to examine the remedy being sought by the defendant in the context of these interlocutory proceedings.

REMEDY

[27] The defendant seeks to restrain the plaintiff in terms of the notice of motion dated May 14, 1999. The factors to be taken into consideration in relation to an injunction are conveniently found in RJR MacDonald Inc. v. Canada (Attorney General), [1994] 1 S.C.R. 312. Shortly stated, these factors are that the applicant must demonstrate a serious question to be tried which limits the Chambers judge to a limited review of the case on the merits. Secondly, considering whether the applicant would suffer irreparable harm

unless the injunction is granted, and thirdly, the balance of convenience (or sometimes described as the balance of inconvenience).

[28] In this overall context, it should also be remembered that an application for an interlocutory injunction is an exercise of an equitable remedy which must take into consideration the conduct of the parties.

[29] In terms of the defendant's applications with reference to the solicitor-client communications which may be on the hard drive of the computer, as previously stated, I am satisfied that those communications are confidential (subject to examination) and that the defendant's claim of privilege should be protected until such time as both parties have an opportunity to make submissions as to the nature and extent of any privilege that should be accorded to any particular document and its possible use in evidence. That claim of privilege, in my view, is of such significance that it should be protected in these interlocutory proceedings. As to the existence of the privilege, there is no doubt that there is a serious question to be tried and the disclosure of this correspondence or drafts of that correspondence prepared and saved on the hard drive may cause the defendant irreparable harm. As to the balance of convenience, in my view, it favours the granting of a limited injunction restraining the plaintiff from accessing the correspondence created by the defendant for the purpose of communications with his solicitors, either matrimonial or commercial.

[30] As to private documents, in my view, the situation is significantly different. For purposes of these reasons as stated, I am prepared to accept that a degree of confidentiality exists and that the defendant had a reasonable expectation of privacy in relation to those documents which were created for family or personal reasons. Nevertheless, the three factors in RJR MacDonald are to be considered in relation to the injunctive relief sought by the defendant. The first factor is whether or not there is a serious question to be tried. In the language of RJR MacDonald, "unless the case on the merits is frivolous or vexatious ... a judge on a motion for relief must, as a general rule, consider the second and third stages of the Metropolitan Stores test." Although the Supreme Court of Canada in Stewart, supra, expressed some reservations as to the extent of the protection of confidential information, in my view, under all the circumstances there is a serious question to be tried as to the nature and extent of the protection of private or personal information which may have been saved on the hard drive.

[31] As to the second test, irreparable harm, it is difficult on the material disclosed to understand how any irreparable harm may be suffered by the defendant. In other words, in answer to the question whether or not a refusal to grant a relief could so adversely affect the defendant's interests to the extent that the harm could not be remedied by the eventual decision on the merits. The answer to that question must be based on the evidence in support of the defendant's application. In the case at bar, I cannot conclude that refusal to grant an injunction restraining the plaintiff in the fashion asked for by the defendant with reference to confidential or private information would result in irreparable harm to the defendant.

[32] Finally, with reference to the third test, the balance of convenience, in this respect it is clear that the balance of convenience favours the plaintiff. The difficulty facing the defendant with reference to the documentation that he has placed on the hard drive of the plaintiff's computer was created by the defendant. The defendant does not come to a court of equity seeking relief with "clean hands". In his attempts to remove personal or

confidential or privileged information from the computer, he did not simply restrict his removal activities to that extent, but went further and removed the software in accordance with his own affidavit and may have significantly impacted the plaintiff's ability to use its computer. There is damage or inconvenience to the plaintiff caused by the defendant. I am satisfied that regarding the private and/or confidential information (not privileged information), the defendant is the author of his own problems; consequently, the balance of convenience militates in favour of not granting the injunction or restraining order sought by the defendant regarding personal or confidential information.

[33] An injunction will issue restraining the plaintiff from using or accessing communications on its computer which were created by the defendant and are communications prepared or sent to the defendant's solicitors, either matrimonial or commercial. The plaintiff will be ordered to keep confidential the contents of any documents inadvertently retrieved. The plaintiff will provide the defendant with a list of all documents that fall within the general privileged category of solicitor-client communications in the event such are accessed.

[34] The injunction may be considered to be unworkable as it allows the plaintiff to use its computer, but at the same time it restrains the plaintiff from accessing portions of the computer with reference to the privileged communications.

[35] The only solution in that respect, in my view, is for the defendant to provide the plaintiff or its solicitors with a list of the dates and the name of the addressee of the documentation that the defendant believes is in the hard drive of the computer and falls within the general class of solicitor-client communication. It is obvious that any memoranda or letter sent by the defendant to his solicitors, either matrimonial or commercial should be in the hands of those solicitors. Under those circumstances, the defendant shall identify with date and addressee, and any file name, the documentation that he believes is caught under the umbrella of privilege. Counsel for the defendant should provide counsel for the plaintiff with that information. One of the terms of the granting of this order is that the information is delivered by the defendant to the plaintiff or its solicitors by December 20, 1999 at close of business. Failing delivery of that information to the solicitors for the plaintiff, the interlocutory injunction will expire and the plaintiff will be at liberty to proceed and access the hard drive of its computer as it sees fit.

[36] An alternative discussed with counsel during the course of this application was the appointment of a third party by the court to vet the contents of the computer under certain terms and conditions which would protect the claims of confidentiality by the defendant subject to the usual discovery of document process. This route is somewhat attractive as it protects the defendant and ultimately allows the plaintiff to use its computer as it sees fit after the process has been completed. No doubt, such a course would be expensive and time consuming and would require cooperation by both the plaintiff and the defendant. If such a course was to be followed, the parties should agree as to the individual to conduct this process, and that individual, in my opinion, should be appointed by the court in order to retain what privilege might be in existence which might otherwise be lost by the introduction of a third party into the process. That might be the subject of a detailed court order setting forth terms and conditions surrounding such activity. In the event the parties prefer that course, I am prepared to hear them further in this respect or alternatively, grant an order on such terms and conditions as counsel may agree to accomplish this end without further application and expense to the parties. I should note, however, that in my

opinion, if such a course is followed all costs associated with that process should be borne by the defendant in any event of the cause and paid forthwith after completion of the process.

[37] The other relief sought by the defendant, however, in my view, is overreaching. The defendant knows what correspondence he has sent to his solicitors. If he does not have copies his solicitors will. There is no justification to order, in my opinion, the plaintiff to list all the documents it has retrieved which would include records, nor to order the plaintiff to deliver copies of same, nor is there any justification in enjoining the plaintiff from copying business documents created by the defendant. Such a blanket order would curtail the plaintiff's access to documents created by the defendant for the plaintiff's business which may form the foundation of a portion of the plaintiff's claim against the defendant.

[38] Moreover, there is no justification in law in the case at bar from restricting the plaintiff's access to its own property.

DISCOVERY OF DOCUMENTS

[39] The plaintiff by its notice of motion dated May 26, 1999 applies for an order relating to discovery of documents that had been or may presently be in the possession of the defendant.

[40] A number of items were requested by the plaintiff in its notice of motion, failing production of which the plaintiff asked that the statement of defence and counterclaim of the defendant be struck out and the proceedings continue as if no such pleading had been filed on behalf of the defendant.

[41] I note that a number of items in the notice of motion in which the plaintiff seeks relief are either dealt with or have been adjourned. For ease of reference according to my note of the exchange between counsel:

Item 1 on the notice of motion is to be adjourned;
Item 3(a) has been completed;
Item 3(b) has been completed insofar as the defendant has produced income tax records. The plaintiff seeks, in addition, however, other financial records which may support income earned by the defendant from March 1996 to the present. Income earned by the defendant is relevant on the issue of his ability to mitigate damages insofar as he may be successful in his wrongful dismissal suit. Consequently, any documentation in the possession of the defendant supporting income should be identified on a list of documents;
Item 3(c), the plaintiff seeks an appropriate property and financial statement apparently prepared by the defendant within his matrimonial proceedings. What is relevant with the claim for wrongful dismissal by the defendant is income produced since the date of his termination. His overall financial circumstances including property or investments that he may have with his spouse are irrelevant; consequently, the application to produce the property and financial statement is dismissed;
Item 3(d), the plaintiff submits that the defendant should produce documentation concerning his employment prospects, earnings or other remunerative activities. On the information before the court, it would appear that the defendant's resume is in the list of

documents. That resume should be identified by date and the list should also encompass all resumes prepared by the defendant as that is relevant again on the issue of mitigation;
Items 3(e), (f), (g) and (h) in my view are irrelevant and need not be listed nor produced by the defendant;
Items 3(i), his income tax returns for 1996, 1997 and 1998 have apparently been produced;
Item 3(j) has been produced.
[42] Consequently, under all the circumstances, any list which the defendant prepares should clearly be exhaustive and should, once he has received the details of his correspondence with his solicitors in this litigation and the matrimonial litigation, identify documents over which he claims privilege. The plaintiff's relief will be limited to the foregoing.

"F. A. Melvin, J."
The Honourable Mr. Justice Melvin

Shoars v. Epson America, Inc.

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION TWO

No. B 073234

ALANA SHOARS,Plaintiff and Appellant

v.

EPSON AMERICA, INC.,Defendant and Respondent.April 14, 1994

1) Plaintiff Alana Shoars appeals from summary judgment in favor of defendant Epson America, Inc. (Epson) in her action for wrongful discharge and slander. We affirm the summary disposition of the first cause of action but reverse with respect to the latter.[FN1]

FN1. When it appeared that a cross-complaint between the parties might still be pending, we requested supplemental information and briefing on the question of appellate jurisdiction. (See California Dental Assn. v. California Dental Hyaienists' Assn. (1990) 222 Cal.App.3d 49, 58-60.) In response, Epson apprised us that although its municipal court action against plaintiff had been consolidated with this case, before entry of judgment the parties had stipulated that the cross-action be dismissed -- without prejudice, and subject to refiling in the event of reversal here. Although the latter provisos could be construed as an effort to contrive an appealable judgment (see id. at pp. 58-59), we conclude that we do have jurisdiction over this appeal, inasmuch as the originally independent cross-action has been dismissed, and there is no assurance it would arise again in this action.

STATEMENT

2) Plaintiff's second amended complaint (complaint) alleged three causes of action. The first, for wrongful discharge, alleged that plaintiff had been employed by Epson to provide training and user support for software use, emphasizing Epson's electronic mail (e-mail) system, which allowed about 700 employees to communicate, through telephone connections, with other computer users outside Epson. Employees accessed the e-mail using personal passwords, and plaintiff had informed them their e-mail was private and confidential.

3) Plaintiff alleged that beginning in August 1989 her supervisor at Epson, Hillseth, acting on Epson's behalf, .tapped. the e-mail, printed it, and read it. Upon discovering this, plaintiff removed some of the printouts from Hillseth's open office, and insisted he cease. Hillseth threatened to fire her if she interfered. Plaintiff nonetheless reported Hillseth's activity to Epson's general manager. Hillseth then had plaintiff fired, on the pretext she had been insubordinate in asking Epson's e-mail manager to provide her a personal outside e-mail line that Hillseth could not access.

4) Plaintiff alleged her termination occurred in retaliation for her reporting of and refusal to go along with Hillseth and Epson's intercepting the e-mail, which in turn violated the public policy and prohibitions concerning wiretapping and eavesdropping stated in Penal Code sections 630-632.5) The complaint alleged a second cause of action under Penal Code section 637.2 (which provides for a private action), to the effect that Hillseth had conspired with Epson's employee relations manager, LaMonte, to use plaintiff's intercepted message requesting a personal e-mail line. In a final cause of action, for slander, plaintiff alleged that just before she was fired, Hillseth and LaMonte falsely told several other Epson employees (plaintiff named eight of them) .that plaintiff had a gun and had threatened to come back into the plant and shoot people..

6) The complaint named Hillseth and LaMonte as defendants along with Epson. Earlier, plaintiff had separately sued Hillseth and LaMonte on the statutory cause of action. Shortly before filing her complaint against all parties, plaintiff had voluntarily dismissed the separate action against Hillseth and LaMonte. Inadvertently or not, the dismissal was taken with prejudice.

7) All defendants generally demurred to the entire complaint. The court sustained the demurrer to the statutory cause of action without leave to amend, but overruled as to the wrongful discharge and slander claims. Defendants then moved for summary judgment, on the theory that the case against Hillseth and LaMonte was barred by res judicata, in light of the dismissal with prejudice, and was similarly barred as against Epson because Epson's alleged liability was based only on the acts of Hillseth and LaMonte. The court granted summary judgment to Hillseth and LaMonte, but denied Epson's motion.

8) Shortly before the trial date, Epson again moved for summary judgment. Epson once more asserted that suit against it was precluded by plaintiff's having dismissed her related action against Hillseth and LaMonte. In addition, Epson challenged the wrongful discharge claim on substantive grounds.

9) Accompanying its motion, Epson filed a .separate statement of undisputed material facts. under Code of Civil Procedure section 437c, subdivision (b) (subdivision (b)), which listed nine such facts, seven of them based upon the contents of the complaint and the court's prior grant of summary judgment to Hillseth and LaMonte. With her opposition, plaintiff provided a separate statement of triable material issues of fact under subdivision (b), which did not, as required, also respond to the facts in Epson's statement.

10) The trial court granted Epson's motion. The minute order of these proceedings stated in part, Here, [plaintiff] has only supplied a 'Statement of Triable Issues of Material Fact and Supporting Evidence.' She has made no attempt to respond to the facts set out by [Epson] in its separate statement. The Court declines to sift through Plaintiff's papers to discern whether there is actually a factual dispute in this case. [FN2]

FN2. The minute order text quoted above may have been prepared by a commissioner, rather than the judge who ruled. But the court seems to have adopted that order; and in any event, a subsequent attorney order which the court signed also referred to and relied upon Plaintiff's failure to oppose any fact in Epson's Separate Statement . . . ..

DISCUSSION

11) Plaintiff contests the summary judgment only on - grounds the court abused its discretion in granting the motion for failure to file a complete separate statement under subdivision (b). We agree that this was not an appropriate case in which to grant summary judgment for that reason. Epson's motion was essentially made on legal grounds, and Epson's undisputed facts, to which plaintiff did not formally respond, largely concerned the existence and contents of the complaint and the order granting summary judgment to Hillseth and LaMonte. Plaintiff's failure to stipulate to these facts on file, while technically inappropriate, did not hinder consideration of the motion. The summary judgment statute fundamentally provides that the motion for summary judgment shall be granted if all the papers submitted show that there is no triable issue as to any material fact and that the moving party is entitled to a judgment as a matter of law. (Code Civ. Proc., 437c, subd. (c), emphasis added.) That legal question, and the subsidiary legal issues raised, were the focus of this motion.

12) But for similar reasons, reversal is not necessarily required. Even assuming the deficient separate statement was why the court granted the motion, the summary judgment must be sustained if correct on any theory presented. (Perez v. 222 Sutter St. Partners (1990? 222 Cal.App.3d 938, 943, fn. 4.) We therefore consider, de novo, the legal basis for the summary judgment. (See ibid.; Saldana v. Globe-Weis Svstems Co. (1991) 233 Cal.App.3d 1505, 1515.)

13) The judgment cannot be sustained on the basis that plaintiff's dismissal with prejudice of her action against Hillseth and LaMonte exonerated Epson. Epson relies on the doctrine that a judgment determining an employee's lack of fault also bars suit against the employer for derivative liability. (E.g., Freeman v. Churchill (1947) 30 Cal.2d 453, 461.) But this doctrine is a species of nonparty collateral estoppel (see 7 Witkin, Cal. Procedure (3d ed. 1985) Judgment, 302, pp. 740-741), which in turn applies only to issues actually litigated and decided in the first action. (People v. Sims (1982) 32 Cal.3d 468, 484.) Here, no issues were determined by plaintiff's voluntary dismissal of the separate action against Hillseth and LaMonte. Whatever its res judicata or retraxit effect as between plaintiff and the individual defendants (see Torrey Pines Bank v. Superior Court (1989) 216 Cal.App.3d 813, 820-821), that dismissal did not create any collateral estoppel running in favor of Epson. (See id. at pp. 825-829 (dis. opn.).)

14) In this light, summary adjudication of plaintiff's third cause of action, for slander, was inappropriate. The alleged statement that plaintiff had a gun and had threatened to return to Epson's plant and shoot people could qualify as slanderous under Civil Code section 46. Although the comments might be conditionally privileged, Epson did not attempt to prove that defense on its motion. [FN3]

FN3. We do not consider other allegedly defamatory statements that are not presently embraced in the pleadings. However, summary adjudication was proper with respect to the wrongful discharge cause of action, based on alleged retaliation for plaintiff's resistance to and reporting a claimed violation of Penal Code section 631 in Hillseth's tapping Epson's e-mail.

15) In a declaration reiterating her complaint, plaintiff, without any showing of personal knowledge, averred that Epson and Hillseth .had placed a tap on the electronic mail gateway where [Epson's] mainframe computer interfaced with the outside MCI E-Mail communications service.. In a responsive declaration, Hillseth stated that in the summer of 1989 Epson began to equip and train its employees with special .Gateway. hardware

and software that allowed Epson's internal e-mail system to access the external, MCI telephonic e-mail system. The Gateway system automatically logged messages sent and received, and could be directed also to .download. the messages to Epson's computer. The system was installed and maintained with this feature activated, to allow technical troubleshooting of the e-mail system. Downloaded messages were automatically erased as new ones were entered. Hillseth declared that he worked with the message file to assist users with problems they reported; in doing so, he printed out and flipped through copies of the messages, to find and read those with which problems were being experienced.

16) The foregoing facts do not present a triable issue that Hillseth or Epson violated Penal Code section 631 (section 631). Section 631 essentially proscribes (1) tapping telephone lines, (2) making unauthorized connections with them, or (3) reading or attempting to learn the contents of a communication, without consent of all parties or in any unauthorized manner, while it is passing over a wire or is being sent from or received at any place in California. (631, subd. (a); Roaers v. Ulrich (1975) 52 Cal.App.3d 894, 898; see Ribas v. Clark (1985) 38 Cal.3d 355, 359-360.). [FN4] Neither plaintiff's nor Hillseth's declarations reflected any tapping or unauthorized connection with a telephone line; the only such line in question -- if any -- was MCI's outside transmission line. And as to the third prohibition, downloading of messages into storage by Epson's computer software did not constitute reading them or attempting to learn their contents. (See Rogers v. Ulrich, supra, at p. 898; cf. People v. Wilson (1971) 17 Cal.App.3d 598, 603.)

FN4. Section 631 was repealed and reenacted without substantive change effective January 1, 1994. The version applicable to the events in suit has been noted for its ambiguity. (E.g., Warden v. Kahn (1979) 99 Cal.App.3d 805, 811.)

17) Plaintiff also sought to bring her complaint about the downloading within other public policy sources. None of these applied either. Penal Code section 632, subdivision (a) prohibits eavesdropping on or recording confidential communications, as defined in Penal Code section 632, subdivision (c), by means of any electronic amplifying or recording device. We do not construe the latter subdivision as rendering e-mail messages sent or received as part of Epson's business .confidential. as to Epson itself. (Cf. People v. Soles (1977) 68 Cal.App.3d 418, 421.) Moreover, Penal Code section 630 and Article I, section 1 of the California Constitution, which more generally declare rights of privacy, cannot reasonably be read to protect against business place conduct that does not violate the particular proscriptions of the adjacent Invasion of Privacy Act sections.

18) Plaintiff's first cause of action therefore was properly subject to summary adjudication. Epson having sought such adjudication as well as summary judgment, we may and shall direct entry of a corresponding order. (See White Motor Corp. v. Teresinski (1989) 214 Cal.App.3d 754, 764, fn. 17.)

DISPOSITION

19) The judgment is reversed. On remand, the trial court shall enter a new order (a) summarily adjudicating that plaintiff's first cause of action has no merit and (b) denying defendant's motion for summary judgment, etc., in all other respects. The parties shall bear their own costs.

NOT FOR PUBLICATION.

J. FUKUTO
We concur:P.J. BORENJ. GATES

TGB Insurance Services Corp. v. Zieminski

TBG INSURANCE SERVICES CORPORATION, Petitioner,

v.

THE SUPERIOR COURT OF LOS ANGELES COUNTY, Respondent;

ROBERT ZIEMINSKI, Real Party in Interest.

No. B153400

In the court of Appeal of the State of California

Second Appellate District

Division One

(Super. Ct. No. BC246390)

ORIGINAL PROCEEDING; petition for a writ of mandate, Alban I. Niles, Judge. Petition granted.

COUNSEL

Paul, Hastings, Janofsky & Walker, Eve M. Coddon and Bradley S. Pauley for Petitioner.

Astor & Phillips, Gary R. Phillips, George R. Phillips, Jr., and Ronald N. Sarian for Real Party in Interest.

No appearance for Respondent.

Filed February 22, 2002

An employer provided two computers for an employee' s use, one for the office, the other to permit the employee to work at home. The employee, who had signed his employer' s "electronic and telephone equipment policy statement" and agreed in writing that his computers could be monitored by his employer, was terminated for misuse of his office computer. After the employee sued the employer for wrongful termination, the employer demanded production of the home computer. The employee refused to produce the computer and the trial court refused to compel production. On the employer' s petition, we conclude that, given the employee' s consent to his employer' s monitoring of both computers, the employee had no reasonable expectation of privacy when he used the home computer for personal matters. We issue the writ as prayed.

FACTS

For about 12 years, Robert Zieminski worked as a senior executive for TBG Insurance Services Corporation. In the course of his employment, Zieminski used two computers

owned by TBG, one at the office, the other at his residence. Zieminski signed TBG' s "electronic and telephone equipment policy statement" in which he agreed, among other things, that he would use the computers "for business purposes only and not for personal benefit or non-Company purposes, unless such use [was] expressly approved. Under no circumstances [could the] equipment or systems be used for improper, derogatory, defamatory, obscene or other inappropriate purposes." Zieminski consented to have his computer "use monitored by authorized company personnel" on an "' as needed' " basis, and agreed that communications transmitted by computer were not private. He acknowledged his understanding that his improper use of the computers could result in disciplinary action, including discharge.

In December 1998, Zieminski and TBG entered a "Shareholder Buy-Sell Agreement," pursuant to which TBG sold 4,000 shares of its stock to Zieminski at $.01 per share; one-third of the stock was to vest on December 1, 1999, one-third on December 1, 2000, and one-third on December 1, 2001, each vesting contingent upon Zieminski' s continued employment; if Zieminski' s employment terminated before all of the shares had vested, TBG had the right to repurchase the non-vested shares at $.01 per share. As part of the buy-sell transaction, Zieminski signed a confidentiality agreement and gave TBG a two-year covenant not to compete. One-third of Zieminski' s shares vested on December 1, 1999. In March 2000, TBG' s shareholders (including Zieminski) sold a portion of their TBG shares to Nationwide Insurance Companies; more specifically, Zieminski sold 1,230 of his 1,333 vested shares to Nationwide for a cash price of $1,278,247.

On November 28, 2000, three days before another 1,333 shares were to vest, Zieminski' s employment was terminated. According to TBG, Zieminski was terminated when TBG discovered that he "had violated TBG' s electronic policies by repeatedly accessing pornographic sites on the Internet while he was at work." According to Zieminski, the pornographic Web sites were not accessed intentionally but simply "popped up" on his computer. Zieminski sued TBG, alleging that his employment had been wrongfully terminated "as a pretext to prevent his substantial stock holdings in TBG from fully vesting and to allow . . . TBG to repurchase [his] non-vested stock" at $.01 per share.

TBG answered and (through its lawyers) asked Zieminski (through his lawyer) to return the home computer and cautioned Zieminski not to delete any information stored on the computer' s hard drive. In response, Zieminski acknowledged that the computer was purchased by TBG and said he would either return it or purchase it, but said it would be necessary "to delete, alter, and flush or destroy some of the information on the computer' s hard drive, since it contains personal information which is subject to a right of privacy." TBG refused to sell the computer to Zieminski, demanded its return without any deletions or alterations, and served on Zieminski a demand for production of the computer. (Code Civ. Proc., § 2031.)[FOOTNOTE 1] Zieminski objected, claiming an invasion of his constitutional right to privacy.

TBG moved to compel production of the home computer, contending it has the right to discover whether information on the hard drive proves that, as claimed by TBG, Zieminski violated his employer' s policy statement. In TBG' s words, Zieminski' s "repeated voluntary and non-work-related access of sexually explicit web-sites is . . . one of the foremost issues in the case. As such, a significant piece of evidence in this action is the [home computer], as its hard drive may confirm that [Zieminski] has, in fact, accessed the same or similar sexually explicit web-sites at home, thereby undermining [Zieminski' s] . . . story that, at work, such sites ' popped up' involuntarily." TBG suggested that, in

light of Zieminski' s agreement to be bound by TBG' s policy statement, and in light of the fact that the home computer belongs to TBG, Zieminski could not seriously claim that he had a reasonable expectation of privacy when he used it for personal matters.

Zieminski opposed the motion, accused TBG of pursuing a "' scorched earth' defense policy," demanded sanctions, and insisted that (notwithstanding the policy statement) he retained an expectation of privacy with regard to his home computer. According to Zieminski, the home computer was provided as a "' perk' " given to all senior executives. He said that, "[a]lthough the home computer was provided so that business related work could be done at home, it was universally accepted and understood by all that the home computers would also be used for personal purposes as well." He said his home computer was used by his wife and children, and that it "was primarily used for personal purposes and contains significant personal information and data" subject to his constitutional right of privacy (including "the details of [his] personal finances, [his] income tax returns," and all of his family' s personal correspondence). Zieminski (who had admitted at his earlier deposition that he had signed the policy statement) did not mention the policy statement in his opposition memorandum or his declaration.[FOOTNOTE 2]

The trial court denied TBG' s motion, finding the information on the computer was "merely corroborative of facts already in [TBG' s] possession; since [TBG] already has extensive evidence, any additional evidence that the [home computer] may disclose does not outweigh the fact that the computer contains personal information." TBG then filed a petition for a writ of mandate, asking us to intervene. We issued an order to show cause and set the matter for hearing.

DISCUSSION

TBG contends it is entitled to inspect Zieminski' s home computer. We agree.

A.

A "party may obtain discovery regarding any matter, not privileged, that is relevant to the subject matter involved in the pending action . . . if the matter either is itself admissible in evidence or appears reasonably calculated to lead to the discovery of admissible evidence." (§ 2017, subd. (a).) "In the context of discovery, evidence is ' relevant' if it might reasonably assist a party in evaluating its case, preparing for trial, or facilitating a settlement. Admissibility is not the test, and it is sufficient if the information sought might reasonably lead to other, admissible evidence." (Glenfed Development Corp. v. Superior Court (1997) 53 Cal.App.4th 1113, 1117.) In the more specific context of a demand for production of a tangible thing, the party who asks the trial court to compel production must show "good cause" for the request -- but unless there is a legitimate privilege issue or claim of attorney work product, that burden is met simply by a fact-specific showing of relevance. (§ 2031, subds. (a)(2), (l); cf. Glenfed Development Corp. v. Superior Court, supra, 53 Cal.App.4th at p. 1117.)

Here, the home computer is indisputably relevant (Zieminski does not seriously contend otherwise),[FOOTNOTE 3] and the trial court' s finding that TBG already has other "extensive evidence" misses the mark. TBG is entitled to discover any non-privileged information, cumulative or not, that may reasonably assist it in evaluating its defense, preparing for trial, or facilitating a settlement. Admissibility is not the test, and it is sufficient if the information sought might reasonably lead to other, admissible

evidence.[FOOTNOTE 4] (Irvington-Moore, Inc. v. Superior Court (1993) 14 Cal.App.4th 733, 738-739 [a party may use multiple methods to obtain discovery and the fact that information was disclosed under one method is not, by itself, a proper basis to refuse to provide discovery under another method].) Zieminski offers no authority to the contrary, and we know of none. The issue, therefore, is whether he has a protectible privacy interest in the information to be found on the computer.

B.

Zieminski' s privacy claim is based on article I, section I, of the California Constitution, which provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." When affirmative relief is sought to prevent a constitutionally prohibited invasion of privacy, the plaintiff must establish "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." (Hill v. National Collegiate Athletic Assn. (1994) 7 Cal.4th 1, 39-40.) Here, we assume the existence of an abstract privacy interest in Zieminski' s financial and other personal information but conclude, by the reasons explained below, that the evidence is insufficient to support the trial court' s implied finding that Zieminski had a reasonable expectation of privacy in the circumstances. As we also explain, the trial court may in any event make such orders as are necessary to minimize TBG' s intrusion.

1.

Assuming the existence of a legally cognizable privacy interest, the extent of that interest is not independent of the circumstances, and other factors (including advance notice) may affect a person' s reasonable expectation of privacy. (Hill v. National Collegiate Athletic Assn., supra, 7 Cal.4th at p. 36.) "A ' reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms," and "the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant." (Id. at p. 37.)[FOOTNOTE 5]

Accordingly, our decision about the reasonableness of Zieminski' s claimed expectation of privacy must take into account any "accepted community norms," advance notice to Zieminski about TBG' s policy statement, and whether Zieminski had the opportunity to consent to or reject the very thing that constitutes the invasion. (Id. at pp. 36, 42.)

(a)

The "community norms" aspect of the "reasonable expectation" element of an invasion of privacy claim is this: "' The protection afforded to the plaintiff' s interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens.' " (Hill v. National Collegiate Athletic Assn., supra, 7 Cal.4th at p. 37, quoting Rest.2d, Torts, § 652D, com. c.) In Hill, where the issue was whether drug testing constituted an invasion of privacy, the "community" was "intercollegiate athletics, particularly in highly competitive postseason championship events," which by their nature involve "close regulation and scrutiny of the physical fitness and bodily condition of student athletes. Required physical examinations

(including urinalysis), and special regulation of sleep habits, diet, fitness, and other activities that intrude significantly on privacy interests are routine aspects of a college athlete' s life not shared by other students or the population at large. . . . [¶] As a result of its unique set of demands, athletic participation carries with it social norms that effectively diminish the athlete' s reasonable expectation of personal privacy in his or her bodily condition, both internal and external." (Hill v. National Collegiate Athletic Assn., supra, 7 Cal.4th at pp. 41-42.)[FOOTNOTE 6]

We are concerned in this case with the "community norm" within 21st Century computer-dependent businesses. In 2001, the 700,000 member American Management Association (AMA) reported that more than three-quarters of this country' s major firms monitor, record, and review employee communications and activities on the job, including their telephone calls, e-mails, Internet connections, and computer files. Companies that engage in these practices do so for several reasons, including legal compliance (in regulated industries, such as telemarketing, to show compliance, and in other industries to satisfy "due diligence" requirements), legal liability (because employees unwittingly exposed to offensive material on a colleague' s computer may sue the employer for allowing a hostile workplace environment), performance review, productivity measures, and security concerns (protection of trade secrets and other confidential information). (American Management Assn., 2001 AMA Survey, Workplace Monitoring & Surveillance, Summary of Key Findings (April 2001) (hereafter "AMA Findings") [as of Feb. 13, 2002]; and see McIntosh, E-Monitoring Workplace.com: The Future of Communication Privacy in the Minnesota Private-Sector Workplace, 23 Hamline L.Rev. 539, 541-542, fn. 10.)

It is hardly surprising, therefore, that employers are told they "should establish a policy for the use of [e-mail and the Internet], which every employee should have to read and sign. First, employers can diminish an individual employee' s expectation of privacy by clearly stating in the policy that electronic communications are to be used solely for company business, and that the company reserves the right to monitor or access all employee Internet or e-mail usage. The policy should further emphasize that the company will keep copies of Internet or e-mail passwords, and that the existence of such passwords is not an assurance of the confidentiality of the communications. [¶] An electronic communications policy should include a statement prohibiting the transmission of any discriminatory, offensive or unprofessional messages. Employers should also inform employees that access to any Internet sites that are discriminatory or offensive is not allowed, and no employee should be permitted to post personal opinions on the Internet using the company' s access, particularly if the opinion is of a political or discriminatory nature." (Fernandez, Workplace Claims: Guiding Employers and Employees Safely In And Out of the Revolving Door (1999) 614 Practicing Law Institute, Litigation and Administrative Practice Course Handbook Series, Litigation 725; see also Gantt, An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace (Spring 1995) 8 Harv. J.L. & Tech. 345, 404-405 [numerous commentators recommend that employers establish corporate policies addressing e-mail privacy, and many employers have done just that].)[FOOTNOTE 7] For these reasons, the use of computers in the employment context carries with it social norms that effectively diminish the employee' s reasonable expectation of privacy with regard to his use of his employer' s computers. (Cf. Hill v. National Collegiate Athletic Assn., supra, 7 Cal.4th at p. 42.)[FOOTNOTE 8]

(b)

TBG' s advance notice to Zieminski (the company' s policy statement) gave Zieminski the opportunity to consent to or reject the very thing that he now complains about, and that notice, combined with his written consent to the policy, defeats his claim that he had a reasonable expectation of privacy.[FOOTNOTE 9]

Several months after Zieminski started using the home computer, he signed TBG' s policy statement, thereby acknowledging his understanding that the home computer was "the property of the Company" and, as such, "to be used for business purposes only and not for personal benefit or non-Company purposes." He agreed that the computer would not "be used for improper, derogatory, defamatory, obscene or other inappropriate purposes," acknowledged his understanding that "communications transmitted by Company systems [were] not considered private," and consented to the Company' s designation of "authorized personnel to enter such systems and monitor messages and files on an ' as needed' basis." He was notified that this monitoring could "include the review, copying or deletion of messages, or the disclosure of such messages or files to other authorized persons." His signature shows that he read the Company' s policy, understood it, and agreed to adhere to it.

As can be seen, Zieminski knew that TBG would monitor the files and messages stored on the computers he used at the office and at home. He had the opportunity to consent to TBG' s policy or not, and had the opportunity to limit his use of his home computer to purely business matters. To state the obvious, no one compelled Zieminski or his wife or children to use the home computer for personal matters, and no one prevented him from purchasing his own computer for his personal use. With all the information he needed to make an intelligent decision, Zieminski agreed to the Company' s policy and chose to use his computer for personal matters. By any reasonable standard, Zieminski fully and voluntarily relinquished his privacy rights in the information he stored on his home computer, and he will not now be heard to say that he nevertheless had a reasonable expectation of privacy. (Hill v. National Collegiate Athletic Assn., supra, 7 Cal.4th at pp. 36, 42; see also Feminist Women' s Health Center v. Superior Court (1997) 52 Cal.App.4th 1234, 1247-1249 [where an employer is not obligated to hire a particular employee, the employee' s consent to even a serious privacy invasion defeats the employee' s claim that she had a reasonable expectation of privacy].)

In his declaration filed in opposition to TBG' s motion to compel production of the home computer, Zieminski states that "it was universally accepted and understood by all [senior executives at TBG] that the home computers would also be used for personal purposes," and that he was never "informed that [he] could not use the home computer for personal purposes, or that [he] should not have an expectation of privacy with respect to the personal contents." His declaration is conveniently silent about the signed TBG policy statement, and about his admission (at his earlier deposition) that he had in fact signed the policy statement, and his self-serving hearsay statements are not corroborated by other TBG employees or by anyone. Under these circumstances, Zieminski' s declaration cannot be viewed as substantial evidence of anything. (Cf. D' Amico v. Board of Medical Examiners (1974) 11 Cal.3d 1, 21-22 [where an admission or concession is obtained not in the normal course of human activities but in the context of an established pretrial procedure whose purpose is to elicit facts, and where such an admission becomes relevant to the determination whether there exists an issue of fact, the admission trumps a subsequent declaration to the contrary].)[FOOTNOTE 10]

2.

As explained above, Zieminski voluntarily waived whatever right of privacy he might otherwise have had in the information he stored on the home computer. But even assuming that Zieminski has some lingering privacy interest in the information he stored on the home computer, we do not view TBG' s demand for production as a serious invasion of that interest. (Hill v. National Collegiate Athletic Assn., supra, 7 Cal.4th at pp. 39-40.) Appropriate protective orders can define the scope of TBG' s inspection and copying of information on the computer to that which is directly relevant to this litigation, and can prohibit the unnecessary copying and dissemination of Zieminski' s financial and other information that has no rational bearing on this case. (See Britt v. Superior Court (1978) 20 Cal.3d 844, 859 [a party' s waiver of his constitutional right to privacy must be narrowly rather than expansively construed, and compelled disclosure should be limited to information "essential to the fair resolution of the lawsuit"]; Vinson v. Superior Court (1987) 43 Cal.3d 833, 842 [a plaintiff cannot be allowed to make serious allegations without affording the defendant an opportunity to put their truth to the test]; cf. Harris v. Superior Court (1992) 3 Cal.App.4th 661, 668; Save Open Space Santa Monica Mountains v. Superior Court (2000) 84 Cal.App.4th 235, 255-256.)

On remand, it will be up to Zieminski to identify with particularity the information that he claims ought to be excluded from TBG' s inspection and copying; it will be up to the trial court to determine whether a protective order should issue and, if so, to determine the scope of the protection and the means by which production will be made (to insure compliance with the trial court' s orders). (§ 2031, subd. (g).) We leave specifics to the parties and to the sound discretion of the trial court. (Valley Bank of Nevada v. Superior Court (1975) 15 Cal.3d 652, 658.)

DISPOSITION

The petition is granted, and a writ will issue, commanding the trial court (1) to vacate its order denying TBG' s demand for production, (2) to enter a new order granting the motion and, following such further briefing and hearing as the court deems necessary and appropriate, (3) to decide the protective order issues. TBG is awarded its costs of these writ proceedings.

VOGEL (MIRIAM A.), J.

We concur: SPENCER, P.J., ORTEGA, J.

February 26, 2002 CALIFORNIA

FN1. All section references are to the Code of Civil Procedure.

FN2. Zieminski' s papers filed in opposition to TBG' s writ petition are similarly silent on the subject of TBG' s policy statement and his acceptance of it. Instead, Zieminski tells us, apropos of nothing, that we "should note" that in June of last year, a Marin County superior court judge overruled a demurrer in a class action alleging that the defendant' s "practice of obtaining individuals' web browsing habits violated California consumers' right to privacy under the California Constitution." Leaving to one side the impropriety of Zieminski' s citation of an unpublished and unpublishable superior court order (Cal. Rules of Court, rules 976, 977), the case is inapposite -- because the alleged invasion of

privacy arises out of the "secret accumulation of . . . private information by an entity with whom [the plaintiffs] have not agreed to deal with . . . ." (See In re Doubleclick Cases (Super. Ct. Marin County, 2001, No. JC4120) 2001 WL 1029646.) As we will explain, Zieminski' s consent defeats his claim that he had a reasonable expectation of privacy.

FN3. TBG contends "the history of Zieminski' s Internet use stored on [his home computer' s] hard drive, including the length of time spent at particular web-sites, [would] constitute unique and accurate evidence that Zieminski' s access of improper non-business and sexually explicit web-sites at work was intentional, not accidental, as Zieminski contends," and that sexually explicit websites, if found on Zieminski' s home computer, would impeach Zieminski' s claim that these sites just "popped up" on his office computer. We agree that, if found on the home computer, this information would be relevant.

FN4. If admissibility mattered, the fact that TBG may have other evidence in its possession is immaterial. There has been no finding that any particular piece of evidence will be admissible, and there is no reason to make such a finding at this stage of the proceedings.

FN5. Although Hill suggests that consent is a complete defense to a constitutional privacy claim (Hill v. National Collegiate Athletic Assn., supra, 7 Cal.4th at p. 40), at least one court of appeal has viewed consent "as a factor in the balancing analysis, and not as a complete defense to a privacy claim." (Kraslawsky v. Upper Deck Co. (1997) 56 Cal.App.4th 179, 193; see also Chin, Cathcart, Aexelrod & Wiseman, Cal. Practice Guide: Employment Litigation (The Rutter Group 2001) ¶ 5:731, p. 5-62.) In the drug testing cases, including Hill and Kraslawsky, the invasion of privacy is far more substantial than in our case. As the Supreme Court explained in Hill, there are two general classes of legally recognized privacy interests: (1) interests in precluding dissemination or misuse of sensitive and confidential information or "informational privacy" ; and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference or "autonomy privacy." (Hill v. National Collegiate Athletic Assn., supra, 7 Cal.4th at p. 35.) There is another significant distinction between the drug cases and our case. When an employer requires drug testing as a condition of employment, the employee must either submit to the invasion of his "autonomy privacy" or, typically, lose his job. When an employer requires consent to computer monitoring, the employee may have his cake and eat it too -- he can avoid any invasion of his privacy by using his computer for business purposes only, and not for anything personal. In the context of the case before us, we view Zieminski' s consent as a complete defense to his invasion of privacy claim. With consent viewed as one of several factors, we would reach the same result -- because the invasion is slight and the need for disclosure great.

FN6. At the time Hill was decided, the Supreme Court recognized that, like "other claims for invasion of the state constitutional right to privacy, future [drug testing] claims arising in the employment context will be subject to the elements and standards [the high court announced in Hill], which require careful consideration of reasonable expectations of privacy and employer, employee, and public interests arising in particular circumstances." (Hill v. National Collegiate Athletic Assn., supra, 7 Cal.4th at pp. 55-56, fn. 20.)

FN7. There can be serious consequences for inattentive employers. (E.g., Cotran v. Rollins Hudig Hall Internat., Inc. (1998) 17 Cal.4th 93; Curtis v. Citibank, N.A. (2d Cir. 2000) 226 F.3d 133; Owens v. Morgan Stanley & Co. (S.D.N.Y. 1997) 1997 WL 403454, 74 Fair Empl. Prac. Cas. (BNA) 876; and see Settle-Vinson, Employer Liability for Messages Sent by Employees Via EMail and Voice Mail Systems (1998) 24 T. Marshall L.Rev. 55.)

FN8. According to the AMA Findings, four out of ten surveyed companies allow employees full and unrestricted use of office e-mail, but "only one in ten allow the same unrestricted access to the internet. Companies are far more concerned with keeping explicit sexual content off their employees' screens than with any other content or matter." (AMA Findings, supra, .) See also, Com. v. Proetto (2001) 771 A.2d 823, 829, 832 [any reasonably intelligent person "savvy enough" to use the Internet is aware that messages are received in a recorded format and can be downloaded or printed by the party receiving the message; by sending a communication over the Internet, the party expressly consents to the recording of the message and demonstrates that he has "no reasonable expectation of privacy in his e-mails"]; Bohach v. City of Reno (D.Nev. 1996) 932 F.Supp. 1232; compare Gantt, An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace, supra, 8 Harv. J.L. & Tech. 345.)

FN9. According to the AMA Findings, "[t]here is a strong correlation between active monitoring practices and formal, written policies covering e-mail, internet, and/or software use. Ninety-five percent of companies that actively monitor employees have written policies, compared with 75% of those that do no monitoring." (AMA Findings, supra, .)

FN10. We summarily reject Zieminski' s assertions (1) that, simply by reason of the computer' s use at his home, his "right of privacy is at its zenith," and (2) that his family' s use of his company-owned computer somehow imbues the information stored on the computer with an aura of privacy that otherwise would not exist. We agree with TBG that, in "today' s portable society, where one' s computer files can be held and transported in the palm of the hand, relevant evidence should not escape detection solely because it was created within the physical confines of one' s home."

Zesta Engineering v. Cloutier

DATE:20021127

DOCKET: C35856

COURT OF APPEAL FOR ONTARIO

FINLAYSON, CHARRON and SIMMONS JJ.A.

B E T W E E N:

ZESTA ENGINEERING LTD.

Timothy Pinos and Jacqueline L. Wall

for the appellants

Plaintiff

(Appellant)

- and -

DAVID CLOUTIER, MICHAEL JEFFERIES, HI-CAP TECHNOLOGIES, GUISEPPE DURANTE, KEITH SANGER, JAMES WHITE and KELVIN TECHNOLOGIES INC.
Douglas Christie and Jill M. Knudsen

for the respondents

Defendants

(Respondents)

A N D B E T W E E N:

DAVID CLOUTIER, GUISEPPE DURANTE, KEITH SANGER and KELVIN TECHNOLOGIES INC.

Plaintiffs by Counterclaim

(Respondents)

-and-

VINCENT EASTMAN, RUTH EASTMAN, MARCEL JONES, DONALD STEPHEN LOCK and ZESTA ENGINEERING LTD.

Defendants to the

Counterclaim

(Appellants)

Heard: September 16 and 17, 2002

On appeal from the judgment of Justice Blenus Wright dated February 22, 2001, reported at [2001] O.J. No. 621, 7C.C.E.L. (3d) 53 (S.C.J.).

ADDENDUM ON COSTS

BY THE COURT:

[1] On October 3, 2002, this court released its reasons for ordering a new trial in this matter and invited counsel to make written submissions as to costs. We have now considered those submissions.

[2] Following the release of our reasons, counsel sought leave to make further submissions on the scope of the new trial, more particularly whether it should include those claims that were not the subject-matter of the proceedings before this court. Leave to make further submissions was refused since this court was of the view that it had adequately addressed all substantive matters in its endorsement. For the guidance of the parties, it is our view that it stands to reason that our order setting aside the trial judgment and ordering a new trial extended only to those claims that formed the subject-matter of the appeal before this court. More particularly, no cross-appeal was taken from a) the award of damages against David Cloutier for secret commissions; b) the dismissal of the counterclaim against Vincent Eastman, Ruth Eastman, Marcel Jones and Donald Stephen Lock; or c) the dismissal of the counterclaim brought by Keith Sanger. Consequently those claims were finally adjudicated upon at the first trial as reflected in paragraphs 1, 2 and 3 of Wright J.'s judgment and that part of the judgment is not affected by the order of this court. It is our view, however, that the execution of paragraph 1 of the judgment in respect to the damage award against David Cloutier should be stayed pending final adjudication on the other claims involving David Cloutier at the new trial.

[3] Counsel also correctly noted in their submissions that a consequence of the order of this court setting aside the trial judgment and ordering a new trial is that the existing costs award of Wright J. with respect to the original trial is also set aside. The appellant seeks an order for its costs of the trial. In our view, it would not be appropriate for this court to make an award of costs in respect of the first trial. Rather, the costs of the first trial will be reserved to the presiding justice at the new trial.

[4] As indicated in our reasons for decision, the appellant is entitled to its costs of the proceedings in this court. Having considered the submissions of the parties, we hereby fix those costs on a partial indemnity basis at $36,000, all inclusive. Our reasons can be briefly stated. We have considered the bills of costs submitted by the appellant. However, we make no specific finding with respect to the amount of time spent or the rates charged by counsel. In our view, the costs award should reflect more what the court views as a fair and reasonable amount that should be paid by the unsuccessful parties rather than any exact measure of the actual costs to the successful litigant. We note however that we have discounted the costs related to the investigation of the new evidence as it is our view that those costs should not form part of the costs award for the proceedings in this court. We note further that the costs are awarded in respect of the motion to introduce fresh evidence only. We do not find it appropriate to make an award of costs in respect of the appeal since it was not heard, or disposed of, on the merits. Nonetheless, in arriving at a reasonable quantum, we have taken into consideration the fact that the motion to introduce fresh evidence could not have been brought by the appellant independently of its appeal.

Released: November 27, 2002

Funds for this study were provided by

The Houston and Calgary Chapters of
ARMA International
In conjunction with
The ARMA International Educational Foundation

The ARMA International Educational Foundation is the non-profit, (501(c)3, affiliate of ARMA International, the primary professional association for the records and information profession in the world.

Mission
The ARMA International Educational Foundation supports education and research initiatives that promote the advancement of both information managers and the information management profession. Recorded information is the lifeblood of the modern organization, but rarely is it treated as a critical asset, primarily because there is little quality research to create the comprehensive body of knowledge required to support information management as a profession. The AIEF purpose is to answer that need by soliciting funds for this research and then providing a vehicle through which conclusions can be tested, documented and communicated to the information management community.

If you found value in this publication, please consider making a financial contribution to the Endowment Fund of the Foundation. This can be accomplished by visiting the Foundation's web site, www.armaedfoundation.org, or by contacting

Foundation Administrator
ARMA Int'l Educational Foundation
1609 Terrie Drive
Pittsburgh PA 15241
USA

Additional information about the Foundation can be found at GuideStar

The National Database of Nonprofit Organizations
http://www.guidestar.org/search/report/gs_report.jsp?ein=31-1556655

Comments about this publication and suggestions for further research are welcome. Please direct your inquiry to the Foundation Administrator.