Filed 2/22/02

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION ONE

TBG INSURANCE SERVICES CORPORATION, Petitioner, v. THE SUPERIOR COURT OF LOS ANGELES COUNTY, Respondent; ROBERT ZIEMINSKI, Real Party in Interest.	No. B153400 (Super. Ct. No. BC246390)

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

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.

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.)[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.

---

[1] All section references are to the Code of Civil Procedure.

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.[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

---

[2] 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.

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),[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.[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

---

[3] 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.

[4] 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.

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.)[5]

---

[5] 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

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

---

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.

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.)[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") <http//:www.amanet.org/research> [as of Feb. 13, 2002]; and see McIntosh, *E-*

---

[6] 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.)

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].)[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.)[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.[9]

---

[7] 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.)

[8] 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,* <http//:www.amanet.org/research>.) 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.)

[9] 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,* <http//:www.amanet.org/research>.)

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].)[10]

---

[10] 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

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

---

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."

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.

CERTIFIED FOR PUBLICATION.

VOGEL (MIRIAM A.), J.

We concur:

SPENCER, P.J.

ORTEGA, J.