FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee,* v. JEFFREY BRIAN ZIEGLER, *Defendant-Appellant.*	No. 05-30177 D.C. No. CR-03-00008-RFC OPINION

Appeal from the United States District Court
for the District of Montana
Richard F. Cebull, District Judge, Presiding

Argued and Submitted
March 6, 2006—Seattle, Washington

Filed August 8, 2006

Before: Diarmuid F. O'Scannlain, Barry G. Silverman, and
Ronald M. Gould, Circuit Judges.

Opinion by Judge O'Scannlain

COUNSEL

David F. Ness, Assistant Federal Defender, Great Falls, Montana, argued the cause for the defendant-appellant. Anthony R. Gallagher, Federal Defender, District of Montana, was on the briefs.

Marcia Hurd, Assistant United States Attorney, Billings, Montana, argued the cause for the plaintiff-appellee. William W. Mercer, United States Attorney, District of Montana, was on the brief.

OPINION

O'SCANNLAIN, Circuit Judge:

We must determine whether an employee has an expectation of privacy in his workplace computer sufficient to suppress images of child pornography sought to be admitted into evidence in a criminal prosecution.

I

A

Frontline Processing ("Frontline"), a company that services Internet merchants by processing on-line electronic payments, is located in Bozeman, Montana.[1] On January 30, 2001, Anthony Cochenour, the owner of Frontline's Internet-service provider and the fiancé of a Frontline employee, contacted Special Agent James A. Kennedy, Jr. of the FBI with a tip that a Frontline employee had accessed child-pornographic websites from a workplace computer.

[1]Although the district court referred to the company as "Front Line," we use the single-word formulation which more frequently appears in the record.

Agent Kennedy pursued the report that day, first contacting Frontline's Internet Technology ("IT") Administrator, John Softich. One of Softich's duties at Frontline was to monitor employee use of the workplace computers including their Internet access. He informed Kennedy that the company had in place a firewall, which permitted constant monitoring of the employees' Internet activities.[2]

During the interview, Softich confirmed Cochenour's report that a Frontline employee had accessed child pornography via the Internet. Softich also reported that he had personally viewed the sites and confirmed that they depicted "very, very young girls in various states of undress." Softich further informed Kennedy that, according to the Internet Protocol address and log-in information, the offending sites were accessed from a computer in the office of Appellant Jeffrey Brian Ziegler, who had been employed by Frontline as director of operations since August 2000. Softich also informed Kennedy that the IT department had already placed a monitor on Ziegler's computer to record its Internet traffic by copying its cache files.[3]

---

[2]A firewall is a piece of "computer hardware or software that prevents unauthorized access to private data (as on a company's local area network or intranet) by outsider computer users (as of the Internet)." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 471 (11th ed. 2003). It can also be "programmed to analyze the network traffic flowing between [a] computer and the Internet"; it then "compares the information it monitors with a set of rules in its database," and "[i]f it sees something not allowed . . . the firewall can block and prevent the action." NEWTON'S TELECOM DICTIONARY 392 (22nd ed. 2006). Further, "[m]ost firewall programs let you adjust the rules to allow certain types of data to flow freely back and forth without interference." *Id.*

[3]A cache is "a computer memory with very short access time used for storage of frequently or recently used instructions or data." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 171 (11th ed. 2003). "[I]nformation is cached by placing it closer to the user or user application in order to make it more readily and speedily available . . . ." NEWTON'S TELECOM DICTIONARY 189 (22nd ed. 2006).

Agent Kennedy next interviewed William Schneider, Softich's subordinate in Frontline's IT department. Schneider confirmed that the IT department had placed a device in Ziegler's computer that would record his Internet activity. He reported that he had "spot checked" Ziegler's cache files and uncovered several images of child pornography. A review of Ziegler's "search engine cache information" also disclosed that he had searched for "things like 'preteen girls' and 'underage girls.' " Furthermore, according to Schneider, Frontline owned and routinely monitored all workplace computers. The employees were aware of the IT department's monitoring capabilities.

B

The parties dispute what happened next. According to testimony that Softich and Schneider provided to a federal grand jury, Agent Kennedy instructed them to make a copy of Ziegler's hard drive because he feared it might be tampered with before the FBI could make an arrest. Agent Kennedy, however, denied that he directed the Frontline employees to do anything. According to his testimony, his understanding was that the IT department had already made a backup copy of Ziegler's hard drive. As the government points out, his notes from the Softich interview say, "IT Dept has backed up JZ's hard drive to protect info." Thinking that the copy had already been made, Kennedy testified that he instructed Softich only to ensure that no one could tamper with the backup copy.

Whatever Agent Kennedy's actual instructions, the Frontline IT employees' subjective understanding of that conversation seems evident from their actions during the late evening of January 30, 2001. Around 10:00 p.m., Softich and Schneider obtained a key to Ziegler's private office from Ronald Reavis, the chief financial officer of Frontline, entered

Ziegler's office, opened his computer's outer casing, and made two copies of the hard drive.[4]

Shortly thereafter, Michael Freeman, Frontline's corporate counsel, contacted Agent Kennedy and informed him that Frontline would cooperate fully in the investigation. Freeman indicated that the company would voluntarily turn over Ziegler's computer to the FBI and thus explicitly suggested that a search warrant would be unnecessary. On February 5, 2001, Reavis delivered to Agent Kennedy Ziegler's computer tower (containing the original hard drive) and one of the hard drive copies made by Schneider and Softich. Schneider delivered the second copy sometime later. Forensic examiners at the FBI discovered many images of child pornography.

C

On May 23, 2003, a federal grand jury handed down a three-count indictment charging Ziegler with receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2); possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B); and receipt of obscene material, in violation of 18 U.S.C. § 1462.[5] At arraignment, Ziegler entered a plea of not guilty.

Ziegler filed several pretrial motions. At issue here is Ziegler's April 23, 2004, motion to suppress the evidence obtained from the search of Ziegler's workplace computer. Ziegler argued that Agent Kennedy, lacking a warrant, vio-

[4]Agent Kennedy explained that this cooperation was the reason he did not pursue a search warrant. He testified, "At this point, counselor, everybody at Frontline Processing is telling me they're going to cooperate, so I'm not going to go in and start serving search warrants on a company if they're going to cooperate. I have no desire to do that."

[5]No explanation appears in the record for the two year, three month interval between delivery of the computer to the FBI and issuance of the indictment. In any event, Ziegler does not raise any issue regarding such delay.

lated the Fourth Amendment by directing the Frontline employees to search his computer. The government argued that the search was voluntary and therefore private in nature.

On August 10, 2004, the district court held a suppression hearing at which Agent Kennedy and Schneider testified.[6] Agent Kennedy, several times, denied that he instructed Softich and Schneider to make a copy of Ziegler's hard drive or to undertake any search in addition to what the employees had already done. Schneider, however, again testified that Kennedy directed him to make a copy of the hard drive. Schneider's account was also reflected in a time-line he had prepared for Kennedy.[7]

On September 8, 2004, the district court entered a written order denying Ziegler's motion to suppress. Importantly, the court made the factual finding that "Agent Kennedy contacted Softich and Schneider on January 30, 2001 and *directed them to make a back-up of Defendant's computer files*" (emphasis added). However, citing *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000), the court ultimately held that Ziegler had

[6]The defense also offered the testimony of a computer forensics expert, but that testimony was not relevant to the motion to suppress.

[7]On appeal, the government attempts to reconcile the contradictory accounts of the January 30, 2001 interview as a case of simple miscommunication. It explains that confusion ensued when Schneider told Agent Kennedy that they were copying Ziegler's cache files onto a second hard drive. Kennedy, whom the government characterizes as not particularly tech-savvy, allegedly understood Schneider to mean that the IT department had already made a copy of Ziegler's entire hard drive. Thus, it suggests that Agent Kennedy's instructions were only that the IT employees should secure the copy he thought had *already* been made.

There is, in short, a factual dispute concerning the extent of the government's involvement in the search and a corresponding legal dispute as to whether that involvement implicates the Fourth Amendment. *See United States v. Miller*, 688 F.2d 652, 658 (9th Cir. 1982). However, we need not address these issues if Ziegler had no reasonable expectation of privacy in any place searched or any item seized. *See, e.g., United States v. Wong*, 334 F.3d 831, 839 (9th Cir. 2003).

no reasonable expectation of privacy in "the files he accessed on the Internet" and therefore denied Ziegler's motion.

Ziegler subsequently entered into a written plea agreement with the government. Pursuant to the agreement, the government agreed to dismiss the child pornography counts in exchange for Ziegler's agreement to plead guilty to the receipt of obscene material. The parties conditioned the plea agreement on Ziegler's ability to appeal the district court's denial of the pretrial motions, including the motion to suppress. A change of plea hearing occurred on September 24, 2004.

On March 4, 2005, the district court sentenced Ziegler to a two-year term of probation and imposed a fine of $1,000. Ziegler timely filed a notice of appeal.

II

Ziegler's sole contention on appeal is that the January 30, 2001 search of his workplace computer violated the Fourth Amendment and, as such, the evidence contained on the computer's hard drive must be suppressed.[8]

A

Ziegler argues that "[t]he district court erred in its finding that Ziegler did not have a legitimate expectation of privacy in his office and computer." He likens the workplace computer to the desk drawer or file cabinet given Fourth Amendment protection in cases such as *O'Connor v. Ortega*, 480 U.S. 709 (1987). Ziegler further contends that the Fourth Circuit's *Simons* case is inapposite. Whereas in *Simons* "the person conducting the search was a network administrator whose purpose was to search for evidence of employee misconduct,"

[8]We review de novo the district court's denial of Ziegler's motion to suppress. *United States v. Noushfar*, 78 F.3d 1442, 1447 (9th Cir. 1996).

in this case "the search was conducted at the behest of Agent Kennedy who was undeniably seeking evidence of a crime."

The government, of course, views the matter quite differently. It contends that the district court's ruling was correct—Ziegler did not have an objectively reasonable expectation of privacy in his workplace computer. The government explains in its brief:

> Society could not deem objectively reasonable that privacy interest where an employee uses a computer paid for by the company; [sic] Internet access paid for by the company, in the company office where the company pays the rent . . . . This is certainly even more so true where the company has installed a firewall and a whole department of people whose job it was to monitor their employee's Internet activity.

As we know, the Fourth Amendment protects people, not places. *Katz v. United States*, 389 U.S. 347, 351 (1967). Although it is often true that "for most people, their computers are their most private spaces," *United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting), the validity of that expectation depends entirely on its context. *Cf. Ortega*, 480 U.S. at 715 ("We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable.").

[1] In that vein, a criminal defendant may invoke the protections of the Fourth Amendment only if he can show that he had a *legitimate* expectation of privacy in the place searched or the item seized. *Smith v. Maryland*, 442 U.S. 735, 740 (1979). This expectation is established where the claimant can show: (1) a subjective expectation of privacy; and (2) an objectively reasonable expectation of privacy. *See id.* (citing *Katz*, 389 U.S. at 351, 361); *United States v. Shryock*, 342 F.3d 948, 978 (9th Cir. 2003). It is Ziegler's burden to prove

both elements. *United States v. Caymen*, 404 F.3d 1196, 1199 (9th Cir. 2005) (citation omitted).

B

[2] The threshold question then is whether Ziegler had a legitimate expectation of privacy in his workplace computer and the files stored therein.[9] If he had no such expectation, we need not consider whether the Frontline employees acted as agents of the government so as to implicate Fourth Amendment protections.

1

The government does not contest Ziegler's claim that he had a *subjective* expectation of privacy in the computer. The use of a password on his computer and the lock on his private office door are sufficient evidence of such expectation. *See*

[9]Ziegler also urges us to suppress the files found on his computer because it was located in his private office. Although an employee may have a legitimate expectation of privacy in his office, here the Frontline employees did not actually search Ziegler's office. They did not violate a privacy expectation in the office generally, such as through "their conduct of a general search," *Mancusi v. DeForte*, 392 U.S. 364, 369 (1968), or video surveillance, *see United States v. Taketa*, 923 F.2d 665, 672-75 (9th Cir. 1991). Neither did they violate some specific realm of privacy, such as a desk or file cabinet "given over to [Ziegler's] exclusive use," *Schowengerdt v. Gen. Dynamics Corp.*, 823 F.2d 1328, 1335 (9th Cir. 1987), in which Ziegler could have kept private papers or effects. *See Ortega*, 480 U.S. at 717-18. Rather, the Frontline employees entered the office merely to gain access to the computer's hard drive. As we discuss below, Frontline policy entitled its personnel to administrative access to the employees' computers, and as such, Softich and Schneider's entry was an "operational realit[y] of [Ziegler's] workplace [that] diminished his legitimate privacy expectations." *Simons*, 206 F.3d at 399; *see also Taketa*, 923 F.2d at 672 (noting that "a valid regulation may defeat an otherwise reasonable expectation of workplace privacy" (citation omitted)); *cf. United States v. Blok*, 188 F.2d 1019, 1020-21 (D.C. Cir. 1951) (holding invalid a search of an employee's desk because the employer itself was not empowered to conduct the search).

United States v. Bailey, 272 F. Supp. 2d 822, 835 (D. Neb. 2003) (citation omitted).

2

But Ziegler's expectation of privacy in his workplace computer must also have been *objectively* reasonable.

a

[3] In *United States v. Simons*, the case upon which the district court relied, the Fourth Circuit reasoned that an employer's Internet-usage policy—which required that employees use the Internet only for official business and informed employees that the employer would "conduct electronic audits to ensure compliance," including the use of a firewall—defeated any expectation of privacy in "the record or fruits of [one's] Internet use." 206 F.3d at 395, 398. A supervisor had reviewed "hits" originating from Simons's computer via the firewall, had viewed one of the websites listed, and copied all of the files from the hard drive. *Id.* at 396. Despite that the computer was located in Simons's office, the court held that the "policy placed employees on notice that they could not reasonably expect that their Internet activity would be private." *Id.* at 398.

[4] As the government suggests, similar circumstances inform our decision in this case. Though each Frontline computer required its employee to use an individual log-in, Schneider and other IT-department employees "had complete administrative access to anybody's machine." As noted, the company had also installed a firewall, which, according to Schneider, is "a program that monitors Internet traffic . . . from within the organization to make sure nobody is visiting any sites that might be unprofessional." Monitoring was therefore routine, and the IT department reviewed the log created by the firewall "[o]n a regular basis," sometimes daily if Internet traffic was high enough to warrant it. Upon their hir-

ing, Frontline employees were apprised of the company's monitoring efforts through training and an employment manual, and they were told that the computers were company-owned and not to be used for activities of a personal nature. Ziegler, who has the burden of establishing a reasonable expectation of privacy, presented no evidence in contradiction of any of these practices. Like Simons, he "does not assert that he was unaware of, or that he had not consented to, the Internet [and computer] policy." *Simons*, 206 F.3d at 398 n.8.

b

[5] Other courts have scrutinized searches of workplace computers in both the public and private context, and they have consistently held that an employer's policy of routine monitoring is among the factors that may preclude an objectively reasonable expectation of privacy. *See Biby v. Bd. of Regents*, 419 F.3d 845, 850-51 (8th Cir. 2005) (holding that no reasonable expectation of privacy existed where a policy reserved the employer's right to search an employee's computer for a legitimate reason); *United States v. Thorn*, 375 F.3d 679, 683 (8th Cir. 2004), *cert. granted and judgment vacated on other grounds by* 543 U.S. 1112 (2005) (holding that a public agency's computer-use policy, which prohibited accessing sexual images, expressly denied employees any personal privacy rights in the use of the computer systems, and provided the employer the right to access any computer in order to audit its use, precluded any reasonable expectation of privacy); *United States v. Angevine*, 281 F.3d 1130, 1133-35 (10th Cir. 2002) (holding that the employer's computer-use policy, which included monitoring and claimed a right of access to equipment, and the employer's ownership of the computers defeated any reasonable expectation of privacy); *Muick v. Glenayre Electronics*, 280 F.3d 741, 743 (7th Cir. 2002) ("Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy . . . ."); *Wasson v. Sonoma County Jr. Coll. Dist.*, 4 F. Supp. 2d 893,

905-06 (N.D. Cal. 1997) (holding that a policy giving the employer "the right to access all information stored on [the employer's] computers" defeated an expectation of privacy).[10]

C

[6] To warrant Fourth Amendment protection, an expectation of privacy must "be one that society is prepared to recognize as 'reasonable.' " *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Accordingly, we note that at least one court has examined the reasonableness of an expectation of privacy in a workplace computer from the standpoint of "community norms." In *TBG Ins. Services Corp. v. Superior Court*, 117 Cal. Rptr. 2d 155, 96 Cal. App. 4th 443 (Cal. Ct. App. 2002), the California Court of Appeal stated:

> 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

[10]We have no trouble distinguishing the cases in which a court has found a reasonable expectation of privacy in a workplace computer. In those cases, the employer failed to implement a policy limiting personal use of or the scope of privacy in the computers, or had no general practice of routinely conducting searches of the computers. *See United States v. Slanina*, 283 F.3d 670, 676-77 (5th Cir. 2002), *vacated on other grounds by* 537 U.S. 802 (2002), *on appeal after remand* 359 F.3d 356 (5th Cir. 2004) (per curiam); *Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001)

> 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).
>
> . . . . 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.

Id. at 161-62, 96 Cal. App. 4th at 451-52. The court, like the others cited above, held that workplace policies, including the employer's entitlement to monitor usage on an "as needed" basis, defeated a claim to a reasonable expectation of privacy in the computer. *Id.* at 163-64, 96 Cal. App. 4th at 452-54.

d

Surely, some lament the general lack of privacy in the modern workplace. *See, e.g.*, Matthew W. Finkin, *Employee Privacy, American Values, and the Law*, 72 CHI.-KENT L. REV. 221, 226 (1996) ("[T]o the extent the reasonableness of the legitimate expectation of privacy is determined on objective grounds, it would rest upon employer policies, practices, or assurances in the matter . . . . [T]his bids fair to eviscerate any claim to privacy at all." (citation omitted)). But in applying the Fourth Amendment we take societal expectations as they are, not as they could or (some think) should be. *See United States v. Silva*, 247 F.3d 1051, 1055 (9th Cir. 2001) (noting that "[t]he reasonableness of an expectation of privacy is evaluated . . . '[by reference] to understandings that are recognized and permitted by society' " (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978))).

[7] Thus, given the nature of our constitutional inquiry, we think the California court's reasoning is compelling. Social

norms suggest that employees are not entitled to privacy in the use of workplace computers, which belong to their employers and pose significant dangers in terms of diminished productivity and even employer liability. Thus, in the ordinary case, a workplace computer simply "do[es] not provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from government interference or surveillance." *Oliver v. United States*, 466 U.S. 170, 179 (1984); *see also Muick*, 280 F.3d at 743 ("[T]he abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible."). Employer monitoring is largely an assumed practice, and thus we think a disseminated computer-use policy is entirely sufficient to defeat any expectation that an employee might nonetheless harbor.

[8] In short, we see no reason to deviate from the reasoning of the cases cited above. The record evidence in this case establishes that the workplace computer was company-owned; Frontline's computer policy included routine monitoring, a right of access by the employer, and a prohibition against private use by its employees.[11] As such, Ziegler had no objectively reasonable expectation of privacy in his workplace computer and thus no standing to invoke Fourth Amendment protection.

[11]We do not hold that company ownership of the computer is alone sufficient to defeat an expectation of privacy. "Fourth Amendment privacy interests do not . . . turn on property interests." *Schowengerdt*, 823 F.2d at 1333 (citations omitted). As always, the issue depends on what expectations may reasonably coexist with that ownership. At the least, we consider the combination of above-noted factors sufficient to defeat an expectation that would confer Fourth Amendment standing. At the same time, we do not hold that *all* the foregoing factors are necessary to defeat an expectation of privacy in a workplace computer.

III

[9] Because the copying of the hard drive on Ziegler's workplace computer violated no reasonable expectation of privacy, we need not assess whether an agency relationship with the FBI existed here, or whether the search was otherwise reasonable.

AFFIRMED.