

United States Court of Appeals, Ninth Circuit.

UNITED STATES of America, Plaintiff-Appellee,
v.
Jeffrey Brian ZIEGLER, Defendant-Appellant.

Filed Aug. 8, 2006.

Before: O'SCANNLAIN, SILVERMAN, and GOULD, Circuit Judges.

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. 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.

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.

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

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)." 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." Further, "[m]ost firewall programs let you adjust the rules to allow certain types of data to flow freely back and forth without interference."

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

. . . 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. . . .

. . . 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.

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.⁴ 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.

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.”

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. 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, violated the Fourth Amendment by directing the Frontline employees to search his computer. . . .

[...]

On September 8, 2004, the district court entered a written order denying Ziegler’s motion to suppress. . . . [C]iting *United States v. Simons*, 206 F.3d 392 (4th Cir.2000), the court ultimately held that Ziegler had no reasonable expectation of privacy in “the files he accessed on the Internet” and therefore denied Ziegler’s motion.

[...]

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.

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). . . .

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*]. Although it is often true that “for most people, their computers are their most private spaces,” the validity of that expectation depends entirely on its context.

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. This expectation is established where the claimant can show: (1) a subjective expectation of privacy; and (2) an objectively reasonable expectation of privacy.

B

The threshold question then is whether Ziegler had a legitimate expectation of privacy in his workplace computer and the files stored therein. 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.

2

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

a

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. 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.”

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 hiring, 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

[...]

c

To warrant Fourth Amendment protection, an expectation of privacy must "be one that society is prepared to recognize as 'reasonable.'" [Katz]. 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 (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 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. 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.

d

Surely, some lament the general lack of privacy in the modern workplace. But in applying the Fourth Amendment we take societal expectations as they are, not as they could or (some think) should be.

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." 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.

In short, we see no reason to deviate from the reasoning of the cases cited above. . . . As such, Ziegler had no objectively reasonable expectation of privacy in his workplace computer and thus no standing to invoke Fourth Amendment protection.

III

Because the copying of the hard drive on Ziegler's workplace computer violated no reasonable expectation of privacy, we [affirm].