IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, **Plaintiff-Appellee,** **vs.** **JEFFREY BRIAN ZIEGLER,** **Defendant-Appellant.**	 **C.A. 05-30177** **D.C. No.: CR 03-08-BU-RFC**

APPELLEE'S RESPONSE TO PETITION FOR REHEARING AND REHEARING EN BANC

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MONTANA

WILLIAM W. MERCER
United States Attorney

MARCIA HURD
ERIC B. WOLFF
Assistant U.S. Attorneys

U.S. Attorney's Office
P.O. Box 1478
Billings, MT 59103
Phone: (406) 657-6101

ATTORNEYS FOR APPELLEE
United States of America

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, **Plaintiff-Appellee,** **vs.** **JEFFREY BRIAN ZIEGLER,** **Defendant-Appellant.**	 **C.A. 05-30177** **D.C. No.: CR 03-08-BU-RFC**

APPELLEE'S RESPONSE TO PETITION FOR REHEARING AND REHEARING EN BANC

PRELIMINARY STATEMENT AND RESPONSE TO APPELLANT'S RULE 35(b) STATEMENT

This Court's opinion is reported at 456 F.3d 1138 (9th Cir. 2006). The United States files this response pursuant to this Court's orders of September 7 and September 25, 2006.

Rehearing en banc is not "necessary to secure and maintain uniformity of the court's decisions," or to address an "overriding need for national uniformity." Fed. R. App. P. 35(b)(1)(A); Circuit Rule 35-1. The only conflict Ziegler cites with respect to this Court's holding that he had no

legitimate expectation of privacy in his workplace computer is an alleged conflict "with the Supreme Court's decision in *Mancusi v. DeForte*, 392 U.S. 364 (1968)." Pet. 2. In the body of the petition, Ziegler also argues that his colleagues' entry into his office was a Fourth Amendment "search" and cites various decisions from this Court and others, which this Court recognized and distinguished. Pet. 10-12. The petition for rehearing should be denied for the following reasons.

First, this Court correctly applied the reasonable expectation of privacy test of *Katz v. United States*, 389 U.S. 347 (1967). Ziegler argues for a "clear distinction" between government employees and private employees, Pet. 5, but such a distinction obviously depends upon the reasonable privacy expectations of the employee (government or private) in a given factual context. There is no legitimate argument that "reasonable expectation of privacy" is not the test, or that analysis of the expectations in the workplace is not the focus. In *Mancusi*, the employer had refused a subpoena, and state officers conducted a general search of the employee's office. The Supreme Court held that the employee had a reasonable expectation that such an intrusion would not occur. This Court correctly emphasized the facts that set Ziegler's case apart from *Mancusi*:

the company owned the computer, provided the Internet access, monitored that access routinely, and accessed his office and computer consistent with office policy. *Ziegler*, 456 F.3d at 1146.

Second, this Court correctly concluded that the entry into Ziegler's office was not a Fourth Amendment "search." *Ziegler*, 456 F.3d at 1143 n.9. Ziegler, again, ignores distinguishing facts, arguing that the Court "authorizes the government to invade a private office, without a warrant, probable cause, or valid consent, and rifle through a citizen's desktop computer." Pet. 13. Ziegler's colleagues merely entered to make a copy of the computer's hard drive to preserve information they had full access to, some of which they had already viewed in prior monitoring. Such actions by a private employer are plainly reasonable, and given the office policies in this case, it was not a Fourth Amendment search.

BACKGROUND

A. The Investigation of Ziegler's Computer Activities.

On January 30, 2001 FBI Special Agent James Kennedy (hereinafter "Agent Kennedy") received a telephone call from Anthony Cochenour. ER 104. Cochenour's fiancee worked at Frontline Processing, a credit card processing company located in Bozeman, Montana. ER 104. She told him

that the IT people at Frontline found that a person at the company was caught by the company's computer firewall accessing child pornography sites. ER 105. Cochenour told Agent Kennedy to contact John Softich, head of Frontline's IT Department. ER 105.

Agent Kennedy called Softich, who confirmed Cochenour's account. ER 105. Softich explained the firewall that constantly monitored their employee's access to the Internet and also alerted IT personnel if an employee was accessing an improper site. ER 106. Softich told Agent Kennedy that the IT personnel had put in a backup procedure to record everything happening on the computer in question. ER 106. He also reported that he had viewed one of the sites accessed and viewed what appeared to be "very, very young girls in various states of undress." ER 106. Softich told Agent Kennedy that William Schneider in Frontline's IT Department also knew about Ziegler's computer. ER 110.

Agent Kennedy asked Schneider about the privacy expectations of employees within the company's computer system. ER 110-11. Schneider said that there was absolutely "no expectation of privacy" on any company computer and that Ziegler, as well as all other company employees, was fully aware of the monitoring capabilities of the IT department and that all

computers were the property of Frontline Processing. ER 111. Schneider and Softich had already placed hard drives on Ziegler's computer to monitor all the traffic coming and going from his computer. ER 129-30.

Following what they thought was a request from Agent Kennedy, Frontline's employees brought Ziegler's computer tower and the hard drives copying Internet traffic to Agent Kennedy for analysis. ER 115. The computer equipment was subsequently logged into evidence and sent to the FBI computer forensic examiner in Salt Lake City. ER 124. Numerous images of child pornography were located on Ziegler's hard drive.

B. Proceedings In The District Court.

On May 23, 2003, the grand jury indicted Ziegler for Receipt of Child Pornography, 18 U.S.C. § 2252A(a)(2) (Count I); Possession of Child Pornography, 18 U.S.C. § 2252A(a)(5)(B); and Receipt of Obscene Matters, 18 U.S. C. § 1462 (Count III). On April 23, 2004, Ziegler moved to suppress the evidence seized from his work computer. He claimed that the FBI directed Softich and Schneider to search his work computer without a warrant in violation of the Fourth Amendment.

On September 7, 2004, the court denied Ziegler's motion to suppress. ER 141-143. The court made a factual finding that Agent

Kennedy directed Softich and Schneider to obtain the hard-drive from Ziegler's office. But the court ruled that Ziegler did not have a reasonable expectation of privacy given the "nature of [his] employment and the precautions taken by Front Line Processing" including their computer firewall and staff monitoring of computer traffic by employees. ER 143. The court relied upon *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000), in support of its ruling. On September 24, 2004, Ziegler pled guilty to Count III and reserved the right to appeal the denial of his suppression motion. ER 146. Ziegler was sentenced to two years probation.

C. This Court's Decision.

On appeal, Ziegler argued that "the search was instigated and directed by law enforcement in a search for evidence of criminal activity," and that the Fourth Circuit's decision in *Simons* was therefore distinguishable. Ziegler's Opening Brief 13. This Court, however, affirmed the district court, holding that Ziegler did not have a reasonable expectation of privacy in his computer files, and that his colleagues' entry into his office to copy the hard drive was not a Fourth Amendment search.

As an initial matter, this Court noted the office policy with respect to monitoring Internet use and noted that courts "have consistently held that

an employer's policy of routine monitoring is among the factors that may preclude an objective reasonable expectation of privacy." *Ziegler*, 456 F.3d at 1144. Moreover, this case was not among those where "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." *Id.* at 1144 n.10.

This Court then turned to whether the privacy interest advocated by Ziegler was one that society is prepared to recognize as reasonable. Approving of the analysis in *TBG Ins. Services Corp. v. Superior Court*, 96 Cal. App. 4th 443 (Cal. Ct. App. 2002), this Court noted the pervasive use of computers in business, and employers' need to monitor that usage for legal compliance, legal liability, performance review, productivity measures and security concerns. This Court concluded that Ziegler did not have a legitimate expectation of privacy given that Frontline owned the computer, controlled access, had a policy of routine monitoring, and also had a prohibition against private use by its employees. *Ziegler*, 456 F.3d at 1146.

As for the entry into Ziegler's office, this Court held that Frontline employees did not conduct a Fourth Amendment "search" of the office. They "entered the office merely to gain access to the computer's hard

drive," which was a matter of office policy and an "operational realit[y]." *Id.* at 1143 n.9 (quoting *Simons*, 206 F.3d at 399).

ARGUMENT

I. This Court Correctly Applied The Reasonable Expectation Of Privacy Test To The Facts Of This Case.

Ziegler is incorrect in arguing that private employees enjoy some favored constitutional test for determining their privacy expectations. The reasonable expectation of privacy test – derived from *Katz* – is the correct test. The key factors – the policies and practices of the employer, and the reasonable expectations of the employees – are the same for both private and government employees. This Court's consideration of those factors squares with established precedent and the record in this case.

A. The Proper Test – As It Was In *Mancusi* – Is Whether Ziegler Had A Reasonable Expectation Of Privacy.

Ziegler essentially argues that since *Mancusi v. DeForte*, 392 U.S. 364 (1968), there has been a "clear distinction between the Fourth Amendment protection accorded government employees and that accorded those who work in the private sector," and that therefore, the particular circumstances of his employment – ownership of the computer, Internet policies, and so forth – are irrelevant. Pet. 5, 10. As Ziegler would

have it, private employees always have greater expectations of privacy, whereas public employees only have a legitimate expectation of privacy under the Fourth Amendment "if a case-by-case analysis of 'the actual office practices and procedures' establishes that the employee can reasonably expect that others will not enter his space." Pet. 8.

On its face, the "clear distinction" between public and private employees that Ziegler alleges is hardly obvious. As a general matter, it is usually government employees who have greater liberty protections simply because a public employer is a state actor, and thus public employees can invoke constitutional rights against employment actions that private employees cannot. *See*, *e.g.*, *Bodett v. CoxCom, Inc.*, 366 F.3d 736, 748 (9th Cir. 2004) ("Cox is a private employer and as such, is not subject to the constitutional strictures applied to state actors by both the federal and Arizona state constitutions."). Due process is a good example, and the Fourth Amendment is no exception.[1] Whereas Ziegler's private employer may invade his personal privacy and search his office without raising a constitutional issue, "[s]earches and seizures by government employers or

[1] *See Perry v. Sindermann*, 408 U.S. 593, 602-03 (1972) (due process); *Skinner v. Railway Labor Executives'* Ass'n, 489 U.S. 602, 614 (1989) (Fourth Amendment).

supervisors . . . are subject to the restraints of the Fourth Amendment." *O'Connor v. Ortega*, 480 U.S. 709 at 715 (1987). The problem in public employment has been to balance the employee's constitutional rights against "the common sense realization that government offices could not function if every employment decision became a constitutional matter." *Connick v. Myers*, 461 U.S. 138, 142 (1983).

It is, thus, counter-intuitive at the outset for Ziegler to emphasize that private employees enjoy greater expectations of privacy than public employees. And, in fact, the only fair reading of *Ortega* is that the Supreme Court sought to provide government employers with some of the employee-management authority that private employers enjoy, as opposed to permitting Fourth Amendment questions to arise in the government workplace even from employment practices that are typical in private employment. As this Court noted in *Schowengerdt v. General Dynamics Corp.*, 823 F.2d 1328, 1333-34 (9th Cir. 1987), the Supreme Court in *Ortega* reversed and remanded a decision of this Court holding "that Ortega's expectation of privacy was reasonable." Issues for remand included whether "actual office practices and procedures" made such an expectation reasonable. *Id.* at 1334 (quoting *Ortega* at 717 (plurality

opinion of O'Connor, J.)). Indeed, in tension with the central claim of his petition for rehearing, Ziegler concedes that "[b]oiled down to its essentials," *Ortega* gave "government the same ability as that held by private employers to ensure the orderly operation of its workplace." Pet. 9.

Ziegler's only authority, then, for the alleged heightened privacy protection for private employees – some test above and beyond analyzing the expectations of employees based upon the policies and practices of the employer – is the finding of a Fourth Amendment violation arising from the search of a private employee's office in *Mancusi*. But as this Court noted, *Mancusi* involved the "general search" of a private office. *Ziegler*, 456 F.3d at 1143 n.9. The employer did not consent to, or perform, the search. It was conducted by New York state officials after the employer had refused to comply with a subpoena for the records. *Mancusi*, 392 U.S. at 365. The Supreme Court analyzed DeForte's reasonable expectations based upon office facts – just as the Supreme Court later analyzed Dr. Ortega's reasonable expectations – and held that "DeForte would have been entitled to expect that he would not be disturbed except by personal or business invitees, and that records would not be taken except with his permission or that of his union superiors." *Id.* at 369. That holding offers no support to

Ziegler, who had no such expectation of resistance to a subpoena, search or seizure by his employer.

Mancusi is a concrete example of a situation where the actions and policies of a private employer create a reasonable expectation of privacy by the employee. This Court recognized that principle in distinguishing cases where "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." *Id.* at 1144 n.10. *Mancusi* is also an example of how the privacy of private employees can be protected by a private employer's decision to resist disclosure to the government.

Nothing in this Court's opinion suggested that employers cannot insist upon a warrant when the government seeks to search or seize the employer's property, or sue successfully for damages if the search or seizure is warrantless and unreasonable. This Court only held that, given the policies and practices of Ziegler's employer, Ziegler does not have "standing to invoke Fourth Amendment protection." *Id.* at 1146. The

employer obviously had standing but chose instead to cooperate.[2] The Supreme Court in *Mancusi* applied the reasonable expectation of privacy test, as did the Court in *Ortega*. This Court correctly chose to apply that test to Ziegler's circumstances.

---

[2]Ziegler cites a 2002 legal education publication by the Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* as supporting the purported "clear distinction" between the lesser rights of government employees when compared to private employees. Pet. 5. Ziegler does not cite any particular page. The Court can view the publication at http://www.cybercrime.gov/s&smanual2002.htm. The discussion of searches at private workplaces is short. It notes that "[p]rivate company employees generally retain a reasonable expectation of privacy in their workplaces" and follows with a one-paragraph section regarding *Mancusi* (p. 40). The next section concerns how "[p]rivate-sector employers and supervisors generally enjoy a broad authority to consent to searches in the workplace" (p. 41). There is no real analysis of situations falling in-between law enforcement barging in when an employer refuses a subpoena (*Mancusi*), and law enforcement obtaining employer consent. This case is in-between but far closer to consent, and the employer's policies diminished any expectations of privacy.

As for public employees, the discussion is longer – unsurprising, given the government's dual role as employer and law enforcer – and does state that "public employees are less likely to retain a reasonable expectation of privacy against government searches at work than are private employees" (p. 44). That is essentially a truism because the government is the employer. Any search by the government-employer will be a search by the government, and the issue of employer consent is largely eliminated. Framed as freedom from *employer* searches, however, private employees may frequently enjoy less real privacy.

B. This Court Correctly Concluded That Ziegler Had No Reasonable Expectation Of Privacy In The Obscene Material Downloaded From The Internet And Stored On His Work Computer.

According to Ziegler, a "private employer's internal regulations have no effect on the assessment of whether the employee enjoys a legitimate expectation of privacy." Pet. 8. In other words, regardless of the rules, warnings, and monitoring policies of an employer, private employees can reasonably believe that their nefarious use of the Internet and company computers is private. Neither common sense nor established Fourth Amendment precedent supports such expectations.

This Court collected cases from other courts that have "consistently held that an employer's policy of routine monitoring is among the factors that may preclude an objectively reasonable expectation of privacy." *Ziegler*, 456 F.3d at 1144. Ziegler does not offer any cases suggesting otherwise with respect to monitoring policies, and thus his petition for rehearing is an invitation to part company with other circuits, thereby thwarting national uniformity as opposed to achieving it.

The Fourth Amendment principle behind the constitutional significance of a monitoring policy is the well-settled point "that a person has no legitimate expectation of privacy in information he voluntarily turns

over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). In *Smith*, the information was dialing information exposed to the phone company. *Smith*, in turn, relied upon *United States v. Miller*, 425 U.S. 435 (1976), where the Court concluded that a bank depositor has no legitimate expectation of privacy in financial information voluntarily conveyed to banks and exposed to their employees in the ordinary course of business.

It is not as if Ziegler brought an obscene book to work in his briefcase and read it at his desk with his office door locked. He used the company computer network to literally dial-up third-party websites and retrieve obscene materials, and that outreach into cyberspace hit the company's network firewall. By using his office computer and the office's computer network, he exposed his actions to third-parties, no different than the exposure to the phone company in *Smith* or the exposure to the bank in *Miller*, and he was forewarned of that exposure through the monitoring policy. In no credible sense was his activity private; it was open to exposure through the policies and practices of the company.

Of course, companies can have policies that differ from Frontline's. That is their choice. Also, companies can choose to resist cooperation or even a subpoena (as occurred in *Mancusi*) and insist upon a warrant. This

Court recognized that it would be a different case if the employer had no policy, or a policy that it did not implement. *Ziegler*, 456 F.3d at 1144 n.10. This Court also recognized that whether companies offer enhanced privacy protections is a question of "social norms," and that this Court will "take social expectations as they are" – which permits those norms to change. *Id.* at 1145. In Ziegler's case, he could not have reasonably expected privacy in his use of the company computer and company network to access and store obscene material.

II. This Court Concluded Correctly That There Was No Fourth Amendment "Search" Of Ziegler's Office.

To retrieve a copy of his hard drive, Frontline employees entered Ziegler's office. In an ironic twist, Ziegler relies upon cases involving searches by government employers of government employees (whom Ziegler earlier claims have less protection) to argue that the entry by Frontline employees into Ziegler's office violates the Fourth Amendment. Pet. 12 and n.2. The argument fails.

As discussed above, "[s]earches and seizures by government employers or supervisors . . . are subject to the restraints of the Fourth Amendment." *Ortega*, 480 U.S. at 715. A government employer may only search without a warrant if justified by "special needs," including "the

efficient and proper operation of the workplace." *Id.* at 723. A government employer may thereby investigate malfeasance and conduct a search that is "reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [employee misconduct]." *Id.* at 725-26 (quotations omitted). The limitations of the "special needs" exception no doubt influence government employment policies – the government's rules of investigation can only go as far as the "special needs" doctrine permits without a warrant – which in turn heightens expectations of privacy in the government workplace. This is an example of the circularity of the "reasonable expectation" test. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001). It is also an example of how government employees enjoy more real privacy than many of their private-sector counterparts, contrary to Ziegler's assertions.

Private employers are unconstrained by a showing of "special needs," and without that burden of justification, their employment policies and practices may in turn diminish expectations of privacy. In either a public or private context, courts have started by evaluating the actual policies and practices of the office. For example, in *Simons* the Fourth Circuit lamented that there was no evidence in the record as to policies

concerning entry of supervisors into Simons' office, and because "*no such policies* were made a part of this record . . . we must assume that none existed." *Simons*, 206 F.3d at 399 n.10 (emphasis in original). Here, "Frontline policy entitled its personnel to administrative access to the computer's hard drive." *Ziegler*, 456 F.3d at 1143. *Simons* is properly distinguished, and there is no conflict in the circuits on this point.

In *Simons*, even though the Fourth Circuit found a reasonable expectation of privacy in the office, it went on to uphold the search as reasonably related to investigating employee malfeasance. *Simons*, 206 F.3d at 400. Frontline, of course, has no obligation to satisfy *Ortega*'s "special needs" formulation. Frontline can access Ziegler's computer, remove it, or sell it on eBay without any justification at all. Frontline can certainly turn it over to law enforcement. *See Georgia v. Randolph*, 126 S. Ct. 1515, 1524 (2006) (discussing *Coolidge v. New Hampshire*, 403 U.S. 443 (1971), and noting that "[a] co-tenant acting on his own initiative may be able to deliver evidence to the police"); *see also id.* at 1542-43 (Thomas, J., dissenting) ("Just as Mrs. Coolidge could, of her own accord, have offered her husband's weapons and clothing to the police without implicating the Fourth Amendment, so too could Mrs. Randolph have

simply retrieved the straw from the house and given it to Sergeant Murray."). But putting aside assistance to law enforcement, if the intrusion in *Simons* was reasonable, the intrusion here was no less reasonable. *See Ortega*, 480 U.S. at 733 (Scalia, J., concurring in the judgment) ("I would hold that government searches to retrieve work-related materials or to investigate violations of workplace rules – searches of the sort that are regarded as reasonable and normal in the private-employer context – do not violate the Fourth Amendment.").

In the end, the core of Ziegler's argument with respect to his privacy interest in his office is simply a return to his opening salvo: treating his situation as no different than the state officers' barging into the private office in *Mancusi* after the employer refused a subpoena. Thus, Ziegler argues that this Court's decision is "disturbing" because "[t]aken to its logical end, it authorizes the government to invade a private office, without a warrant, probable cause, or valid consent, and rifle through a citizen's desktop computer." Pet. 13. That argument ignores this Court's emphasis upon the particular employer policies in this case, the fact that they were executed by Frontline employees, as well as the broader recognition of social norms subject to change. "Judges and lawyers live on the slippery

slope of analogies; they are not supposed to ski it to the bottom." *Buckley v. American Constitutional Law Foundation, Inc.*, 525 U.S. 182, 195 n.16 (1999) (quoting R. Bork, THE TEMPTING OF AMERICA: THE POLITICAL SEDUCTION OF THE LAW 169 (1990)). Ziegler's closing depiction of this case is certainly at the bottom of the slope, as he ignores pretty much every distinguishing feature that this Court carefully explained.

CONCLUSION

For the foregoing reasons, panel rehearing and rehearing en banc should be denied.

DATED this 5th day of October, 2006.

WILLIAM W. MERCER
United States Attorney

_____
ERIC B. WOLFF
Assistant U.S. Attorney

CERTIFICATE OF SERVICE BY MAIL

The undersigned hereby certifies that she is an employee in the Office of the United States Attorney for the District of Montana, and that on the ____ day of October, 2006, she mailed a true and correct copy of the foregoing Response to Petition for Rehearing and Rehearing En Banc of the United States of America, postage prepaid, to the following addressee(s):

David F. Ness
Federal Defenders of Montana
P.O. Box 3547
Great Falls, MT 59403-3547
Attorney for Defendant-Appellant
Ziegler

_____
Amy R. Weston
Legal Assistant

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 35 and Ninth Circuit Rule 40-1, the attached response to petition for panel rehearing/petition for rehearing en banc is proportionately spaced, has a typeface of 14 points or more, and the body of the argument contains 3,968 words.

WILLIAM W. MERCER
United States Attorney

_____

ERIC B. WOLFF
Assistant U.S. Attorney