NO. 54966-9-I

IN THE COURT OF APPEALS
OF THE STATE OF WASHINGTON
DIVISION I

STATE OF WASHINGTON

Appellant,

v.

ROBERT T. WESTBROOK

Respondent

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF RESPONDENT

Lee Tien
Kevin S. Bankston
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)

Suzanne Lee Elliott, WSBA #12634
705 Second Avenue, Suite 1300
Seattle, WA 98104
(206) 623-0291

Attorneys for Amicus Curiae
Electronic Frontier Foundation

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Law Review Articles and Treatises

IDENTITY AND INTEREST OF AMICUS

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization working to protect individual rights in the digital world. EFF actively encourages and challenges industry and government to support free expression and privacy in the information society. Founded in 1990, EFF is based in San Francisco. EFF has members all over the United States and maintains one of the most-linked-to Web sites in the world, http://www.eff.org.

STATEMENT OF THE CASE

Mr. Westbrook turned his computer over to Gateway Computer for servicing on October 13, 2003. While the computer was being serviced, the service technician viewed some of the files on the computer and discovered that some of the files contained child pornography. The technician informed his manager of the discovered files, and the manager contacted the police.

An officer arrived at Gateway Computer and the technician showed her Mr. Westbrook's computer. The officer then opened some of the files listed on the on-screen menu and discovered that they contained child pornography. After the officer viewed several such images, the computer was seized and a warrant to search the entire computer was obtained based on the statements of the technician and the officer who had viewed the files.

I. ARGUMENT

The Electronic Frontier Foundation, on behalf of Respondent

Robert Westbrook, urges this Court to affirm the holding of the trial court: t a computer user does not relinquish his expectation of privacy in the contents of a personal computer merely by having that computer serviced by a third party.

A personal computer may contain a "world of very private and potentially embarrassing information:" a diary, an archive of personal and business e-mails, tax returns, and an almost-infinite range of other material. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV.L.REV. at 1 (forthcoming 2006) (draft of August 3, 2005), *available at* http://ssrn.com/abstract=697541. It even contains "much more information that you didn't even know existed, such as websurfing records indicating every website you visited and every search engine query you entered for the past twelve months." *Id*. In short, a computer may contain a vast amount of personal data about its user; data that the user may prefer not to reveal to government agents or any other persons.

At the same time, a personal computer is a notoriously fickle device. Computer users may encounter a wide range of problems, ranging from software bugs that impair the normal its normal functioning to viruses or hardware failures that render the computer completely unusable. Many computer users are unable to address such problems on their own and need to seek outside assistance to remedy these problems. In addition, users may be unable to remove any sensitive information from the computer before seeking professional assistance, either because the computer is completely unusable and the data cannot be accessed at all, or

because they lack knowledge of the data's existence or the means of removing the data. *See, e.g., id.* at 12-13; Christopher Wall and Jason Paroff, *Cracking the Computer Forensics Mystery*, UTAH BAR J. 10-11 (October, 2004) (discussing the methods by which user-deleted files may be recovered through computer forensics: "[a]t the heart of computer forensics is the idea that within the electronic realm of evidence, delete does not really mean delete.").

When a computer user turns her computer over to a technician for servicing without first removing all private information from the computer, what are the legal consequences? Is the user necessarily exposing all of the information contained on the computer to governmental inspection? Or does the user still retain the right to prevent inspection of the data on the computer in the absence of a search warrant or exigent circumstances?

The right to privacy from government inspection is embodied in the Fourth Amendment to the United States Constitution and Article 1, section 7 of the Washington State Constitution. Under the Fourth Amendment, citizens have the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. A search under the Fourth Amendment occurs "if the police intrude into affairs in which a person has a reasonable expectation of privacy." *State v. Kealey*, 80 Wn.App. 162, 167 (1995). The fundamental Fourth Amendment question presented here is whether Mr. Westbrook possessed a reasonable expectation of privacy, "i.e., one rooted

in understandings that are recognized and permitted by society," in the contents of his computer even after the computer was submitted to a technician for servicing. *Id.* at 170 (internal quotation marks omitted).[1]

Article 1, Section 7 of the Washington State Constitution states that "[n]o person shall be disturbed in his private affairs … without authority of law." An inquiry under Article 1, section 7, which "is broader than under the Fourth Amendment to the United States Constitution, … focuses on 'those privacy interests which citizens of this state have held, and should be expected to hold, safe from governmental trespass.'" *State v. Jackson*, 150 Wash.2d 251, 259 (2003) (quoting *State v. Myrick*, 102 Wash.2d 506, 511 (1984)). In the present case, the question presented is whether citizens of this state "have held, and should be expected to hold," a privacy interest in the data stored on their personal computers even when that computer is released to a technician for servicing. *Id.*

This Court should hold that a computer owner retains a reasonable expectation of privacy, and a valid privacy interest, in the contents of a computer, even where the computer is submitted to a technician for servicing. To hold otherwise would force a computer user into an unenviable dilemma: forego the manifold advantages of using her

---

[1] In addition to the requirement that an expectation of privacy be objectively reasonable, the expectation must be subjectively held by the defendant. *See, e.g.*, *Kealey*, 80 Wn.App. at 169. However, since the record does not address the matter, this court should assume that Mr. Westbrook did hold such an expectation. *See* Brief of Respondent at 10-11.

computer for any private records, communications or other activities, or abandon her constitutional right of privacy as to any data stored on her computer whenever she submits the computer to another person for service. It would deny the fact that the contents of a personal computer are inherently personal, and deserve the full protection of the state and federal Constitution from government inspection.

The Court should be particularly hesitant to overturn the decision of the trial court in light of the limited record available. The courts have not yet reached any form of consensus with regard to the Fourth Amendment protections afforded to digital data. *See* Kerr, *supra*, at n.4, n.5 and accompanying text. The lack of clarity as to the standard service procedure and any interaction between Mr. Westbrook and Gateway prior to the police examination of files on Mr. Westbrook's computer render it difficult for this court to accurately assess the facts of the case. *See* Brief for Respondent at 4-7. In light of this, the court should be very hesitant to proceed where the State has failed to develop an adequate record.

Therefore, this court should affirm the trial court ruling and suppress all evidence resulting from the warrantless search of the contents of Mr. Westbrook's computer.

A. The contents of Robert Westbrook's computer were protected by the Fourth Amendment and by Article 1, section 7 of the Washington State Constitution.

A personal computer, such as that possessed by Mr. Westbrook, contains a broad range of private files and therefore carries an objectively reasonable expectation of privacy under the Fourth Amendment. In

Kealey, the Court of Appeals held that a woman had an objectively reasonable expectation of privacy in the contents of her purse. *See* 80 Wn.App. at 170. In doing so, it noted that "the very purpose of a purse is to serve 'as a repository for personal, private effects,'" and thus held that a purse by its nature carried a reasonable expectation of privacy. *Id*. (quoting *Arkansas v. Sanders*, 442 U.S. 753, 762 n.9 (1979)). In *State v. Nordlund,* the Court of Appeals noted that "the modern day repository of a man's records, reflections, and conversations" in holding that the data stored on a computer carries the same constitutional protection. 113 Wn.App. 171, 181-82 (2002) (internal quotation marks omitted).

Furthermore, the type of information contained on a personal computer falls squarely within the broader privacy protections granted by Article 1, section 7. In *State v. Jackson*, the Washington Supreme Court held that the attachment of a GPS tracking device to the defendant's vehicle without a warrant constituted a violation of the defendant's privacy interest in his whereabouts. 150 Wash.2d. at 262. The *Jackson* Court noted that the potential access of "information concerning a person's associations, contacts, finances, or activities is relevant in deciding whether an expectation of privacy an individual has is one which a citizen of this state should be entitled to hold," and that the "intrusion into private affairs made possible with a GPS device is quite extensive as the information obtained can disclose a great deal about an individual's life." *Id*. at 260, 263 (citations omitted). The information stored on a computer fits squarely with these concerns.

B. Mr. Westbrook did not relinquish his constitutional rights by submitting his computer to a technician for service.

As discussed above, a personal computer, such as that owned by Mr. Westbrook, contains a vast array of private information, and is therefore protected from warrantless police searches. Mr. Westbrook did not forfeit this protection merely by seeking professional assistance in servicing his computer.

Allowing limited access to a private area does not in and of itself eliminate an objectively reasonable expectation of privacy in that area. In *Stoner v. State of California*, the Supreme Court confirmed that a person had an objectively reasonable expectation of privacy in a hotel room, even where hotel staff had express or implied permission to enter the room for specific tasks. 376 U.S. 483 (1964). Similarly, in *Chapman v. United States*, the Supreme Court held that an objectively reasonable expectation of privacy remained in a leased apartment where the landlord possessed a key and had the right to enter the premises for limited purposes including building inspections and maintenance. 365 U.S. 610 (1961).

Furthermore, in Washington, even information necessarily disclosed to a third party does not constitute a complete relinquishment of a privacy interest in that information. In *State v. Gunwall*, the Supreme Court of Washington held that a defendant retained a reasonable expectation of privacy in dialed telephone numbers where those numbers were necessarily provided to the telephone company for other purposes. 106 Wash.2d 54 (1986). The court stated that "[t]he concomitant

disclosure to the telephone company, for internal business purposes, of the numbers dialed by the telephone subscriber does not alter the caller's expectation of privacy and transpose it into an assumed risk of disclosure to the government." *Id.* at 67. The defendant therefore did not relinquish his privacy interest because the "disclosure [of telephone numbers to the telephone company was] necessitated because of the nature of the instrumentality, but more significantly the disclosure has been made for a limited business purpose and not for release to other persons for other reasons." *Id.* at 68.

Relinquishing possession of an object does not necessarily eliminate constitutional privacy protections associated with that object. In *United States v. Most*, the court held that a person retained a reasonable expectation of privacy in the contents of a plastic bag temporarily left with a grocery store clerk. 876 F.2d 191 (D.C. Cir. 1989). And in *State v. Boland*, the Supreme Court of Washington held that the defendant retained a privacy interest in the contents of opaque trash bags left on the curb for pickup. 115 Wash.2d 571 (1990). The *Boland* court noted that "[w]hile … an expectation that children, scavengers, or snoops will not sift through one's garbage is unreasonable, average persons would find it reasonable to believe the garbage they place in their trash cans will be protected from warrantless governmental intrusion." *Id*. at 578.

In this case, Mr. Westbrook retained a reasonable expectation of privacy in the contents of his computer when he submitted the computer to a technician for service. The practical necessity of turning a computer over

to a service technician, like the necessity of allowing other persons into a hotel room or leased apartment for maintenance purposes, did not render a continuing expectation of privacy unreasonable. Nor was Mr. Westbrook's expectation of privacy eliminated when he temporarily relinquished physical control over the computer. The record gives no indication that he had reason to expect that the files on his computer would be opened and viewed in the course of the requested service.[2] Furthermore, even if he did realize that the computer repairman could possibly "snoop" on the contents of his computer, *Boland* holds that he did not thereby relinquish his entire privacy interest in those contents. Instead, even after relinquishing physical control over the computer to the Gateway technician, Mr. Westbrook retained a reasonable expectation that the contents of his computer "[would] be protected from warrantless governmental intrusion." *Id.*

II. CONCLUSION

This court should recognize that Mr. Westbrook has a reasonable expectation of privacy in the contents of his computer, even where the computer was submitted to a technician for service. This court should

---

[2] In their brief, Appellants assert that the technician was required to actually view the files on the hard drive in the course of performing the requested services; however, this assertion is not supported in the record. *See* Opening Brief for Appellant at 15-16; Brief for Respondent at 5-6.Nor is viewing individual files necessary to copy the data on a hard drive or to confirm that the copy was successful. *See* BRIAN CARRIER, FILE SYSTEM FORENSIC ANALYSIS 47-69 (2005) (describing methods by which the data on a computer can be copied without opening any files).

therefore affirm the trial court ruling.

Dated: August 12, 2005 Respectfully submitted,

_____

Lee Tien
Kevin S. Bankston
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)

Suzanne Lee Elliott, WSBA #12634
705 Second Avenue, Suite 1300
Seattle, WA 98104
(206) 623-0291

Attorneys for Amicus Curiae
Electronic Frontier Foundation