

RECEIVED
SUPREME COURT
STATE OF WASHINGTON

2007 APR 10 P 3: 18

NO. 78946-1 BY RONALD R. CARPENTER

SUPREME COURT OF THE STATE OF WASHINGTON

HANS YORK and KATHERINE YORK, parents of AARON E. YORK
and ABRAHAM P. YORK, and SHARON A. SCHNEIDER and
PAUL A. SCHNEIDER, parents of TRISTAN S. SCHNEIDER,

Appellants,

v.

WAHKIAKUM SCHOOL DISTRICT 200,

Respondent.

AMENDED AMICUS BRIEF OF THE STATE OF WASHINGTON

ROBERT M. MCKENNA
Attorney General

Karin Nyrop, WSBA 14809
Assistant Attorney General
University of Washington Division

Shannon Inglis, WSBA 23164
Assistant Attorney General
Criminal Justice Division

Carol Murphy, WSBA 21244
Deputy Solicitor General
P.O. Box 40100
Olympia, WA 98504-0100
(360)664-9018
Attorneys for Amicus Curiae
State of Washington

FILED
SUPREME COURT
STATE OF WASHINGTON
2007 APR 10 1:54 PM
BY RONALD R. CARPENTER

ORIGINAL

TABLE OF CONTENTS

I.	IDENTITY AND INTEREST OF AMICUS CURIAE	1
II.	ISSUE PRESENTED	2
III.	ARGUMENT	3
A.	Article 1, Section 7 Of The Washington State Constitution Is No More Expansive Than The Fourth Amendment To The United States Constitution In The Context Of Student-Athlete Drug Testing	3
1.	There Is No Precedent For The Assertion That Article 1, Section 7 Confers Greater Privacy Rights To Student-Athletes Subject To Random Drug Tests	3
2.	Application Of The <i>Gunwall</i> Factors Does Not Favor More Expansive Rights To Student Athletes In This Context	5
3.	The Special Needs Exception Applies Equally Under The Fourth Amendment And Article 1, Section 7	8

TABLE OF AUTHORITIES

Cases

<i>Bd. of Educ. of Indep. Sch. Dist. 92 of Pottawatomie Cy. v. Earls</i> , 536 U.S. 822, 122 S. Ct. 2559, 153 L. Ed. 2d 735 (2002).....	9, 13
<i>Bedford v. Sugarman</i> , 112 Wn.2d 500, 772 P.2d 486 (1989).....	4, 5
<i>Chandler v. Miller</i> , 520 U.S. 305, 117 S. Ct. 1295, 137 L. Ed. 2d 513 (1997).....	9
<i>Darrin v. Gould</i> , 85 Wn.2d 859, 540 P.2d 882 (1975).....	7
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67, 121 S. Ct. 1281, 149 L. Ed. 2d 205 (2001).....	10
<i>Fusato v. Washington Interscholastic Activities Ass'n</i> , 93 Wn. App. 762, 970 P.2d 774 (1999).....	7
<i>Griffin v. Wisconsin</i> , 483 U.S. 868, 107 S. Ct. 3164, 97 L. Ed. 2d 709 (1987).....	10
<i>Henderson v. City of Simi Valley</i> , 305 F.3d 1052, (9th Cir. 2002)	10
<i>In re Juveniles A, B, C, D, E</i> , 121 Wn.2d 80, 847 P.2d 455 (1993).....	9, 10, 11, 12
<i>In re Meyer</i> , 142 Wn.2d 608, 16 P.3d 563 (2001).....	4
<i>Ino Ino, Inc. v. City of Bellevue</i> , 132 Wn.2d 103, 937 P.2d 154 (1997).....	5
<i>MacWade v. Kelly</i> , 460 F.3d 260 (2nd Cir. 2006)	14

<i>Murphy v. State</i> , 115 Wn. App. 297, 62 P.3d 533.....	6
<i>Murphy v. State</i> , 149 Wn.2d 1035, 75 P.3d 968 (2003).....	6
<i>New Jersey v. T.L.O.</i> , 469 U.S. 325, 105 S. Ct. 733, 83 L. Ed. 720 (1985).....	10
<i>O'Hartigan v. Dep't of Pers.</i> , 118 Wn.2d 111, 821 P.2d 44 (1991).....	5
<i>Rise v. Oregon</i> , 59 F.3d 1556 (9th Cir. 1995)	11
<i>Robinson v. City of Seattle</i> , 102 Wn. App. 795, 10 P.3d 452 (2000).....	11, 12
<i>Sanchez v. Cy. of San Diego</i> , 464 F.3d 916 (9th Cir. 2006)	10
<i>Skinner v. Railway Labor Executives' Ass'n</i> , 489 U.S. 602, 109 S. Ct. 1402, 103 L. Ed. 2d 639 (1989).....	9, 12
<i>State v. Brooks</i> , 43 Wn. App. 560, 718 P.2d 837 (1986).....	3, 6
<i>State v. Davis</i> , 125 Wn. App. 59, 104 P.3d 11 (2004).....	10
<i>State v. Farmer</i> , 116 Wn.2d 414, 805 P.2d 200 (1991).....	11
<i>State v. Gunwall</i> , 106 Wn.2d 54, 720 P.2d 808 (1986).....	4, 5, 6, 7, 8
<i>State v. Houser</i> , 95 Wn.2d 143, 622 P.2d 1218 (1980).....	8
<i>State v. Johnson</i> , 128 Wn.2d 431, 909 P.2d 293, (1996).....	6, 8

<i>State v. Ladson</i> , 138 Wn.2d 343, 979 P.2d 833 (1999).....	4
<i>State v. Olivas</i> , 122 Wn.2d 73, 856 P.2d 1076 (1993).....	5, 10
<i>State v. Parker</i> , 139 Wn.2d 486, 987 P.2d 73 (1999).....	4
<i>State v. Surge</i> , 122 Wn. App. 448, 94 P.3d 345 (2004).....	10
<i>Taylor v. Enumclaw Sch. Dist. 216</i> , 132 Wn. App. 688, 133 P.3d 492 (2006).....	4, 7
<i>Theodore v. Delaware Valley Sch. Dist.</i> , 575 Pa. 321, 836 A.2d 76 (2003).....	2
<i>Treasury Employees v. Von Raab</i> , 489 U.S. 656, 109 S. Ct. 1384, 103 L. Ed. 2d 685 (1989).....	9
<i>United States v. Heckenkamp</i> , No. 05-10322, slip op. 3877 (9th Cir. Apr. 5, 2007)	10
<i>United States v. Kincade</i> , 379 F.3d 813 (9th Cir. 2004)	11
<i>United States v. Scott</i> , 450 F.3d 863 (9th Cir. 2006)	10
<i>Vernonia Sch. Dist. 47J v. Acton</i> , 515 U.S. 646, 115 S. Ct. 2386, 132 L. Ed. 2d 564 (1995).....	passim
<i>York v. Wahkiakum School District 200</i> , 110 Wn. App. 383, 40 P.3d 1198, <i>review denied</i> , 147 Wn.2d 1010 (2002).....	12
<i>Young Americans for Freedom v. Gorton</i> , 91 Wn.2d 204, 588 P.2d 195 (1978).....	2

Statutes

RCW 28A.600.230..... 7

RCW 28A.600.240(2)..... 7

RCW 43.43.754 10

RCW 70.24.340(1)(a) 10

Other Authorities

Charles Feeney Knapp, *Drug Testing and the Student-Athlete: Meeting the Constitutional Challenge*, 76 Iowa L. Rev. 107 2

Jere Longman, *Drugs in Sports; An Athletes Dangerous Experiment*, *New York Times* (November 26, 2003)..... 2

NCAA Division I Manual, Bylaw 3.2.4.7.1, <https://goomer.ncaa.org/wdbctx/LSDBi/LSDBI.home> 2

NCAA Study of Substance Use Habits of College Student-Athletes, Presented to: the National Collegiate Athletic Association Committee on Competitive Safeguards and Medical Aspects of Sports, June 2001 2

Constitutional Provisions

Const. art. I, § 7..... 3

Const. art. III, § 21 1

I. IDENTITY AND INTEREST OF AMICUS CURIAE

This amicus curiae brief is filed by the Attorney General on behalf of the State of Washington. The Attorney General is the chief legal officer of the State of Washington. Const. art. III, § 21. The State has important interests in this case in the proper interpretation of the constitution and the appropriate balance of governmental interests and the constitutional rights of all Washington citizens.

State agencies represented by the Attorney General include law enforcement agencies, such as the Washington State Patrol and other agencies that possess some law enforcement authority, as well as state colleges and universities that have student athletic programs.

This case implicates important state interests in protecting the health, safety, and welfare of student athletes. Drug use by high school and college athletes poses a unique and significant problem. The compelling force of athletic competition often drives athletes to use drugs to improve performance and gain a competitive edge. Athletes may also use drugs to prevent fatigue, mask pain, and cope with stress. Substance abuse by student-athletes can result in significant injury to the user, as well as the user's teammates, and opponents. Furthermore, the use of performance-enhancing drugs can result in inequitable competitive advantage. Charles Feeney Knapp, *Drug Testing and the Student-Athlete:*

Meeting the Constitutional Challenge, 76 Iowa L. Rev. 107; *see also*, *Theodore v. Delaware Valley Sch. Dist.*, 575 Pa. 321, 836 A.2d 76 (2003) (“with regard to student athletes and drivers, the risk of immediate physical harm to the drug and alcohol user or those with whom he/she is playing a sport or sharing a highway is particularly high”).¹

The public also has an interest in the proper balancing of: individual privacy interests and governmental interests in preventing drug abuse in these circumstances. The Attorney General’s constitutional and statutory powers include the submission of amicus curiae briefs on matters that affect the public interest. *See Young Americans for Freedom v. Gorton*, 91 Wn.2d 204, 212, 588 P.2d 195 (1978).

II. ISSUE PRESENTED

In the context of random drug testing of student athletes, is article 1, section 7 of the Washington Constitution more expansive than the Fourth Amendment to the United States Constitution?

¹ A study by the National Collegiate Athletic Association (NCAA) identified the dangers involved in substance abuse. *See* NCAA Study of Substance Use Habits of College Student-Athletes, Presented to: the National Collegiate Athletic Association Committee on Competitive Safeguards and Medical Aspects of Sports, June 2001; *see also* Jere Longman, *Drugs in Sports: An Athletes Dangerous Experiment*, *New York Times* (November 26, 2003). Based on this study and earlier studies, the NCAA has implemented random drug testing, the purpose of which is to maintain the integrity of the competition and protect the safety of athletes. Failure to consent to the NCAA testing program will result in a student being ineligible to play. NCAA Division I Manual, Bylaw 3.2.4.7.1, <https://goomer.ncaa.org/wdbctx/LSDBi/LSDBI.home> (last visited Apr. 9, 2007).

III. ARGUMENT

A. **Article 1, Section 7 Of The Washington State Constitution Is No More Expansive Than The Fourth Amendment To The United States Constitution In The Context Of Student-Athlete Drug Testing**

1. **There Is No Precedent For The Assertion That Article 1, Section 7 Confers Greater Privacy Rights To Student-Athletes Subject To Random Drug Tests**

The United States Supreme Court has concluded that random drug testing of student-athletes is reasonable under the Fourth Amendment. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 115 S. Ct. 2386, 132 L. Ed. 2d 564 (1995). While in some instances the Washington constitution does afford a person broader rights than those granted by the federal constitution, no authority has held that article 1, section 7 confers greater privacy rights on student-athletes. In fact, the Court of Appeals has concluded that article 1 section 7 affords students no greater protection from searches by school officials than is guaranteed by the Fourth Amendment. *State v. Brooks*, 43 Wn. App. 560, 568, 718 P.2d 837 (1986). This Court should follow the ruling by the Court of Appeals in *Brooks*.

The Yorks attempt to expand the scope of the state constitutional provision which states that “[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law.” Const. art. 1, § 7. While other cases have found article 1, section 7 to provide greater protection against search and seizure in the context of law enforcement activities, that context is remote from this case. It is well established that

the *Gunwall* analysis is context specific. *Bedford v. Sugarman*, 112 Wn.2d 500, 507, 772 P.2d 486 (1989). For instance, in *State v. Ladson*, 138 Wn.2d 343, 348, 979 P.2d 833 (1999), upon which the Yorks rely, a criminal defendant claimed a greater privacy right in the context of search and seizure during a traffic stop. *Ladson's* analysis does not apply to this case, where the privacy right is asserted outside the context of a law enforcement search and seizure. In the context of random drug testing of student athletes, such as the policy at issue here, the potential negative consequence of a positive test is not criminal prosecution but the loss of the privilege to participate in school athletic programs. Participation in interscholastic sports is a privilege, not a right. *Taylor v. Enumclaw Sch. Dist.* 216, 132 Wn. App. 688, 697, 133 P.3d 492 (2006).

The Yorks also cite *State v. Parker*, 139 Wn.2d 486, 493 n.2, 987 P.2d 73 (1999), for the broad proposition that article 1, section 7 provides greater constitutional protection in all possible contexts. In fact, such an expansion of the holding in *Parker* would be contrary to other precedent. This Court has explicitly recognized that the Washington Constitution has the same boundaries as those guaranteed by the federal constitution when analyzing the *Gunwall* factors for a claimed privacy right not involving searches and seizures by law enforcement. *In re Meyer*, 142 Wn.2d 608, 619-20, 16 P.3d 563 (2001), (“the right to privacy guaranteed by the Washington Constitution in this setting has the same boundaries as that guaranteed by the federal constitution”), citing *Ino Ino, Inc. v. City of*

Bellevue, 132 Wn.2d 103, 124, 937 P.2d 154 (1997)); *see also O'Hartigan v. Dep't of Pers.*, 118 Wn.2d 111, 117-18, 821 P.2d 44 (1991).

No court in this state has found that student-athletes have a greater right to privacy under the Washington Constitution than under the federal constitution. It is notable that all cases cited by the Yorks in support of heightened privacy rights arise in the context of law enforcement searches. *See* Appellants' Br. at 19 n.3. Student athletes actually have a limited right to privacy in the context of this case.

2. Application Of The *Gunwall* Factors Does Not Favor More Expansive Rights To Student Athletes In This Context

This Court has consistently declined to engage in an independent state constitutional analysis unless there has been a thorough briefing of the factors listed in *State v. Gunwall*, 106 Wn.2d 54, 58, 720 P.2d 808 (1986). *State v. Olivas*, 122 Wn.2d 73, 82, 856 P.2d 1076 (1993). Additionally, the *Gunwall* analysis must be "specific not just to the individual constitutional provision that is invoked, but also to the sort of right that is asserted." *Bedford v. Sugarman*, 112 Wn.2d 500, 507, 772 P.2d 486 (1989). This Court has not previously analyzed the *Gunwall* factors in relation to a student-athlete's privacy right in this context.

The six criteria in the required *Gunwall* analysis are: (1) the textual language of the state constitution; (2) significant differences in the texts of parallel provisions of the federal and state constitutions; (3) state constitutional and common-law history; (4) preexisting state law;

(5) differences in structure between the federal and state constitutions; and (6) matters of particular state interest or local concern. *Gunwall*, 106 Wn.2d at 65-67. Because prior case law has analyzed the language and structural differences between the state and federal constitutions, the factors pertaining to those differences need not be further analyzed by this court. *State v. Johnson*, 128 Wn.2d 431, 445, 909 P.2d 293, (1996). The remaining factors, preexisting state law (factor 4) and matters of particular state or local concern (factor 6) support an interpretation of the state constitutional right to privacy here co-extensive with the Fourth Amendment.

Preexisting state law recognizes that privacy expectations of student athletes are limited. In fact, the court of appeals has already held that “article 1, section 7 affords students no greater protection from searches by school officials than is guaranteed by the Fourth Amendment.” *State v. Brooks*, 43 Wn. App. 560, 568, 718 P.2d 837 (1986). There is no sound reason to reverse the holding in *Brooks*. Additionally, the holding in *Brooks* is consistent with the ruling in *Murphy v. State*, 115 Wn. App. 297, 62 P.3d 533, *review denied*, *Murphy v. State*, 149 Wn.2d 1035, 75 P.3d 968 (2003), interpreting the privacy protection of article 1, section 7 within the context of the particular case—disclosure of confidential prescription records—to be co-extensive with the Fourth Amendment.

Participation in interscholastic athletics is not a private activity, and the student-athletes who participate voluntarily subject themselves to

some degree of regulation inherent in such participation. There is no fundamental right to participate in interscholastic sports. *Darrin v. Gould*, 85 Wn.2d 859, 873, 540 P.2d 882 (1975). Participation in interscholastic sports is a privilege, not a right. *Taylor v. Enumclaw Sch. Dist.* 216, 132 Wn. App. 688, 697 (2006); *Fusato v. Washington Interscholastic Activities Ass'n*, 93 Wn. App. 762, 768, 970 P.2d 774 (1999). A student who refuses to participate in a random drug testing program only risks losing his or her privilege to participate in interscholastic sports. That risk does not involve a fundamental right and is outweighed by the school's interest in keeping students safe.

Even the statute York cites for the proposition that state law recognizes some privacy rights for students, recognizes that those privacy rights are diminished. *See* RCW 28A.600.230, .240(2) (school officials may search student belongings without a warrant based upon a reasonable belief that the student possesses contraband). Thus, consideration of the fourth *Gunwall* factor, preexisting state law, favors co-extensive state and federal constitutional rights in the context of student-athlete drug tests.

The sixth *Gunwall* factor, whether the matter is of particular state interest or local concern, also favors an interpretation of article 1, section 7 consistent with the Fourth Amendment. The Brief of Respondents explains that local school boards have legitimate interests in regulating the conduct of public school students, and the local school district should be given deference when doing so. Resp't Br. at 22-24. That may be so, but the deference afforded to a local school board does not assist in the

analysis of the sixth factor under *Gunwall*. While the state and local governments certainly have strong concerns on both sides of this issue—privacy, education, the prevention of drug abuse, and participation in extracurricular athletics—those interests are also at play on a national level.

In summary, this Court's analysis of the *Gunwall* factors applied to this context does not support privacy rights more expansive than those granted by the federal constitution. Therefore, this matter should be determined on the basis of federal constitutional standards, relying upon *Vernonia School District 47J*, 515 U.S. 646, not on independent state constitutional grounds.

3. The Special Needs Exception Applies Equally Under The Fourth Amendment And Article 1, Section 7

Both the Fourth Amendment to the United States Constitution and article 1, section 7 of the Washington Constitution prohibit searches absent a warrant based upon probable cause. *State v. Johnson*, 128 Wn.2d 431, 446-47, 909 P.2d 293 (1996). There are, however, a number of exceptions to the warrant requirement. *See State v. Houser*, 95 Wn.2d 143, 149, 622 P.2d 1218 (1980). "For searches outside the criminal context, the Supreme Court has developed the special needs doctrine. This doctrine applies when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *In re Juveniles A, B, C, D, E*, 121 Wn.2d 80, 91, 847 P.2d

455 (1993) (citing *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 619, 109 S. Ct. 1402, 103 L. Ed. 2d 639 (1989)) (internal quotation marks omitted). Application of the special needs exception requires a fact-specific inquiry, considering: 1) the nature of the privacy interest involved; 2) the character of the governmental intrusion; and 3) the nature and immediacy of the government's concerns, and the efficacy of its policy in meeting those concerns. *Bd. of Educ. of Indep. Sch. Dist. 92 of Pottawatomie Cy. v. Earls*, 536 U.S. 822, 830-34, 122 S. Ct. 2559, 153 L. Ed. 2d 735 (2002); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 654-60, 115 S. Ct. 2386, 132 L. Ed. 2d 564 (1995).

The United States Supreme Court has considered whether drug testing programs satisfy the special needs exception on several occasions. The Court sustained drug testing for railway employees involved in train accidents (*Skinner*, 489 U.S. 602), for United States Customs Service employees seeking promotion to certain sensitive positions (*Treasury Employees v. Von Raab*, 489 U.S. 656, 109 S. Ct. 1384, 103 L. Ed. 2d 685 (1989)), and for high school students participating in interscholastic sports (*Vernonia*, 515 U.S. 646; *Earls*, 536 U.S. 822). The Court has struck down drug testing for candidates for state offices, *Chandler v. Miller*, 520 U.S. 305, 117 S. Ct. 1295, 137 L. Ed. 2d 513 (1997), and expectant

mothers, *Ferguson v. City of Charleston*, 532 U.S. 67, 121 S. Ct. 1281, 149 L. Ed. 2d 205 (2001).²

The special needs exception to the warrant requirement also is recognized under Washington law. Applying the special needs exception, this Court has sustained DNA testing upon conviction of certain offenses (former RCW 43.43.754), *State v. Olivas*, 122 Wn.2d 73, 856 P.2d 1076 (1993), and HIV testing upon conviction of certain offenses (RCW 70.24.340(1)(a)), *In re Juveniles A, B, C, D, E*, 121 Wn.2d 80. The court of appeals has also used the special needs exception to sustain DNA testing upon conviction of certain offenses (current RCW 43.43.754). *State v. Surge*, 122 Wn. App. 448, 94 P.3d 345 (2004), *review granted*, 153 Wn.2d 1008 (2005); *see State v. Davis*, 125 Wn. App. 59, 69, 104 P.3d 11 (2004) (same).³

² The United States Supreme court has also applied the special needs exception to uphold searches in other contexts. *See e.g., Griffin v. Wisconsin*, 483 U.S. 868, 873, 107 S. Ct. 3164, 97 L. Ed. 2d 709 (1987) (search of probationer's home). The Ninth Circuit has also utilized the special needs exception. *See e.g., United States v. Heckenkamp*, No. 05-10322, slip op. 3877 (9th Cir. Apr. 5, 2007) (search of university student's computer); *Sanchez v. Cy. of San Diego*, 464 F.3d 916, 925-28 (9th Cir. 2006) (home visits of welfare recipients); *Henderson v. City of Simi Valley*, 305 F.3d 1052, 1056-61 (9th Cir. 2002) (entry into home while daughter retrieves belongings under California domestic violence protection act). *But see United States v. Scott*, 450 F.3d 863, 872 (9th Cir. 2006) (rejecting pre-trial drug testing under special needs analysis).

The term "special needs" first appeared in Justice Blackmun's concurrence in *New Jersey v. T.L.O.*, 469 U.S. 325, 351-53, 105 S. Ct. 733, 83 L. Ed. 720 (1985) (search of high school student's purse). *See Ferguson*, 532 U.S. at 75 n.7.

³ The constitutionality of the current version of RCW 43.43.754 is pending before this Court in *Surge*. Subsequent to the *Surge* Court of Appeals opinion, an en banc Ninth Circuit Court of Appeals affirmed the constitutionality of the federal DNA

In *Robinson v. City of Seattle*, 102 Wn. App. 795, 816, 10 P.3d 452 (2000), the court of appeals declined to apply the special needs exception in the context of drug testing of city applicants for employment, stating that the State Supreme Court “has developed a different approach for article 1, section 7 analysis of governmental searches outside the context of law enforcement.” The *Robinson* Court was incorrect in attributing its independent grounds analysis to *In re Juveniles A, B, C, D, E* and *State v. Farmer*, 116 Wn.2d 414, 428-31, 805 P.2d 200 (1991), because the “privacy interest” considered in those cases was not in the context of search and seizure but in the context of the broader right to privacy. See *In re Juveniles A, B, C, D, E*, 121 Wn.2d at 96-98; *Farmer* 116 Wn.2d, at 428-31.⁴ In fact, in *In re Juveniles A, B, C, D, E*, the Court considered the

statute in *United States v. Kincaid*, 379 F.3d 813 (9th Cir. 2004), *cert. denied*, 544 U.S. 924 (2005). The *Kincaid* Court relied on the reasoning of its opinion in *Rise v. Oregon*, 59 F.3d 1556 (9th Cir. 1995) (totality of the circumstances), rather than the special needs exception.

⁴ The *Farmer* Court explained:

The United States Supreme Court recognizes such a fundamental right of privacy to exist in matters relating to freedom of choice regarding one’s personal life. See *Boddie v. Connecticut*, 401 U.S. 371, 91 S. Ct. 780, 28 L. Ed. 2d 113 (1971). We recognize a similar right to privacy to emanate from the specific guarantees of the Bill of Rights, from the language of the First, Fourth, Fifth, Ninth and Fourteenth Amendments, as well as from article 1, section 7 of the Washington Constitution. *In re Colyer*, 99 Wn.2d 114, 119-20, 660 P.2d 738 (1983) (citing *Griswold v. Connecticut*, 381 U.S. 479, 484, 85 S. Ct. 1678, 14 L. Ed. 2d 510 (1965)).

Farmer, 116 Wn.2d at 429.

constitutionality of the search under the Fourth Amendment, applying the special needs exception. *In re Juveniles A, B, C, D, E*, 121 Wn.2d at 90-96.

In *York v. Wahkiakum School District 200*, 110 Wn. App. 383, 40 P.3d 1198, *review denied*, 147 Wn.2d 1010 (2002),⁵ the court of appeals articulated a test that was slightly different from the *Vernonia* test, and concluded that *Robinson* had in fact applied the test. *Id.* at 386. The *York* Court combined the first two elements of the *Vernonia* test—the nature of the privacy interest, and the character and degree of government intrusion, and then articulated a slightly different third element—“whether a compelling state interest justifies the intrusion and whether the intrusion is a narrowly tailored means of serving the interest.” *Id.*; *c.f. Vernonia*, 515 U.S. at 654-60. Although courts considering the special needs exception have used the term “compelling” in referring to the government interest, *see, e.g., Skinner*, 489 U.S. at 628, the *Vernonia* Court suggested caution in the use of this phrase:

It is a mistake . . . to think that the phrase “compelling state interest,” in the Fourth Amendment context, describes a fixed, minimum quantum of governmental concern, so that one can dispose of a case by answering in isolation the question: Is there a compelling state interest here? Rather,

⁵ *York*, 110 Wn. App. 383, is the same cause of action that is currently before the Court in the present case. *York* was an appeal from the trial court’s denial of the Yorks’ motion for preliminary injunction pending trial in this case. *Id.* at 384.

the phrase describes an interest that appears *important enough* to justify the particular search at hand, in light of other factors that show the search to be relatively intrusive upon a genuine expectation of privacy. Whether that relatively high degree of government concern is necessary in this case or not, we think it is met.

Vernonia, 515 U.S. at 661.

It is true that this Court and the court of appeals have only applied the special needs exception in cases considered under the Fourth Amendment. That is because article 1, section 7 and the Fourth Amendment are co-extensive where a search is not being conducted for law enforcement purposes, not because the special needs exception somehow would be inconsistent with analysis under article 1, section 7. Even if the Court decides that article 1, section 7 affords greater protection than the Fourth Amendment (and it should not), this Court still should use the special needs test. Its fact specific inquiry in each case is entirely compatible with article 1, section 7, regardless of whether that provision is interpreted to provide greater protection to individual privacy in the instant circumstances. *See, e.g., Earls*, 536 U.S. at 830 (*Vernonia* “did not simply authorize all school drug testing, but rather conducted a fact-specific balancing of the intrusion on the children’s Fourth Amendment rights against the promotion of legitimate governmental interests”).

In summary, this Court already recognizes the special needs exception, and it need only consider the facts of the present case and determine whether those facts satisfy the requirements of the exception. *See, e.g., MacWade v. Kelly*, 460 F.3d 260 (2nd Cir. 2006) (random searches of baggage of passengers traveling on New York subways upheld under the special needs exception). However, in the event this Court determines that article 1, section 7 affords greater protection than the Fourth Amendment in the present context, the special needs exception still provides the appropriate analytical framework.

V. CONCLUSION

Based on the foregoing, the State of Washington respectfully urges the Court to recognize that article 1, section 7 is no more expansive than the Fourth Amendment in the context of random drug testing of student athletes.

RESPECTFULLY SUBMITTED this 10th day of April, 2007.

ROB MCKENNA
Attorney General


Karin Nyrop, WSBA 14809
Assistant Attorney General
Shannon Inglis, WSBA 23164
Assistant Attorney General
Carol Murphy, WSBA 21244
Deputy Solicitor General
P.O. Box 40100
Olympia, WA 98504-0100
(360)664-9018
Attorneys for Amicus Curiae
State of Washington

United States v. Heckenkamp
No. 05-10322, slip op. 3877 (9th Cir. Apr. 5, 2007)

FOR PUBLICATION
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,
v.
JEROME T. HECKENKAMP,
Defendant-Appellant.

No. 05-10322
D.C. No.
CR-03-20041-JW

UNITED STATES OF AMERICA,
Plaintiff-Appellee,
v.
JEROME T. HECKENKAMP,
Defendant-Appellant.

No. 05-10323
D.C. No.
CR-00-20355-JW
OPINION

Appeal from the United States District Court
for the Northern District of California
James Ware, District Judge, Presiding

Argued and Submitted
August 17, 2006—San Francisco, California

Filed April 5, 2007

Before: William C. Canby, Jr., Michael Daly Hawkins, and
Sidney R. Thomas, Circuit Judges.

Opinion by Judge Thomas

COUNSEL

Benjamin Coleman, San Diego, California, for the appellant.

Hanley Crew, Assistant United States Attorney, San Francisco, California, for the appellee.

OPINION

THOMAS, Circuit Judge:

In this case, we consider whether a remote search of computer files on a hard drive by a network administrator was justified under the "special needs" exception to the Fourth Amendment because the administrator reasonably believed the computer had been used to gain unauthorized access to confidential records on a university computer. We conclude that the remote search was justified.

Although we assume that the subsequent search of the suspect's dorm room was not justified under the Fourth Amendment, we conclude that the district court's denial of the

suppression motion was proper under the independent source exception to the exclusionary rule.

I

In December 1999, Scott Kennedy, a computer system administrator for Qualcomm Corporation in San Diego, California, discovered that somebody had obtained unauthorized access to (or "hacked into," in popular parlance) the company's computer network. Kennedy contacted Special Agent Terry Rankhorn of the Federal Bureau of Investigation about the intrusion.

Kennedy was able to trace the intrusion to a computer on the University of Wisconsin at Madison network, and he contacted the university's computer help desk, seeking assistance. Jeffrey Savoy, the University of Wisconsin computer network investigator, promptly responded to Kennedy's request and began examining the university's system. Savoy found evidence that someone using a computer on the university network was in fact hacking into the Qualcomm system and that the user had gained unauthorized access to the university's system as well. Savoy was particularly concerned that the user had gained access to the "Mail2" server on the university system, which housed accounts for 60,000 individuals on campus and processed approximately 250,000 emails each day. At that time, students on campus were preparing for final exams, and Savoy testified that "the disruption on campus would be tremendous if e-mail was destroyed." Through his investigation of the Mail2 server, Savoy traced the source of intrusion to a computer located in university housing. The type of access the user had obtained was restricted to specific system administrators, none of whom would be working from the university's dormitories.

Savoy determined that the computer that had gained unauthorized access had a university Internet Protocol ("IP") address¹

¹An IP address is a standard way of identifying a computer that is connected to the Internet. An IP address is comprised of four integers less than 256 separated by periods.

that ended in 117. In addition, Savoy determined that Heckenkamp, who was a computer science graduate student at the university, had checked his email from that IP address 20 minutes before and 40 minutes after the unauthorized connections between the computer at the IP address ending in 117, the Mail2 server, and the Qualcomm server. Savoy determined that the computer at that IP address had been used regularly to check Heckenkamp's email account, but no others. Savoy became extremely concerned because he knew that Heckenkamp had been terminated from his job at the university computer help desk two years earlier for similar unauthorized activity, and Savoy knew that Heckenkamp "had technical expertise to damage [the university's] system."

Although Savoy was confident that the computer that had gained the unauthorized access belonged to Heckenkamp, he checked the housing records to ensure that the IP address was assigned to Heckenkamp's dorm room. The housing department initially stated that the IP address corresponded to a different room down the hall from Heckenkamp's assigned room. The housing department acknowledged that the records could be inaccurate but stated that they would not be able to verify the location of the IP address until the next morning. In order to protect the university's server, Savoy electronically blocked the connection between IP address 117 and the Mail2 server.

After blocking the connection, Savoy contacted Rankhorn. After Savoy informed Rankhorn of the information he had found, Rankhorn told Savoy that he intended to get a warrant for the computer, but he did not ask Savoy to take any action or to commence any investigation.

Later that night, Savoy decided to check the status of the 117 computer from home because he was still concerned about the integrity of the university's system. He logged into the network and determined that the 117 computer was not attached to the network. However, Savoy was still concerned

that the same computer could have "changed its identity," so he checked the networking hardware to determine if the computer that was originally logged on at the 117 address was now logged on at a different IP address. His search confirmed that the computer was now logged on at an IP address ending in 120.

Based on this discovery, Savoy became even more concerned that the Mail2 server "security could be compromised at any time," particularly because "the intruder at this point knows that he's being investigated" and might therefore interfere with the system to cover his tracks. Savoy concluded that he needed to act that night.

Before taking action, Savoy wanted to verify that the computer logged on at 120 was the same computer that had been logged on at 117 earlier in the day. He logged into the computer, using a name and password he had discovered in his earlier investigation into the 117 computer. Savoy used a series of commands to confirm that the 120 computer was the same computer that had been logged on at 117 and to determine whether the computer still posed a risk to the university server. After approximately 15 minutes of looking only in the temporary directory, without deleting, modifying, or destroying any files, Savoy logged off of the computer.

Savoy then determined that "[the 120] machine need[ed] to get off line immediately or as soon as possible" based on "a university security need." He contacted both Rankhorn and a Detective Scheller, who worked for the university police. Savoy informed them of his discoveries and concerns. Rankhorn asked Savoy to wait to take action because he was attempting to get a search warrant. However, Savoy felt that he needed to protect the university's system by taking the machine off line immediately. Therefore, he made the decision to coordinate with the university police to take the computer off line and to "let [the] university police coordinate with the FBI."

Together with Scheller and other university police officers, Savoy went to the room assigned to Heckenkamp.² When they arrived at the room, the door was ajar, and nobody was in the room. Savoy and Scheller entered the room and disconnected the network cord attaching the computer to the network. Savoy noted that the computer had a screen saver with a password, which prevented him from accessing the computer. In order to be sure that the computer he had disconnected from the network was the computer that had gained unauthorized access to the Mail2 server, Savoy wanted to run some commands on the computer. Detective Scheller located Heckenkamp, explained the situation and asked for Heckenkamp's password, which Heckenkamp voluntarily provided.

Savoy used the password to run the commands on the computer and verified that it was the computer used to gain the unauthorized access. After Savoy confirmed that he had the right computer, Scheller advised Heckenkamp that he was not under arrest, but Scheller requested that Heckenkamp waive his Miranda rights and give a statement. Heckenkamp waived his rights in writing and answered the investigator's and detectives' questions. In addition, Heckenkamp authorized Savoy to make a copy of his hard drive for later analysis, which Savoy did. At no time did Savoy or Scheller search Heckenkamp's room. Throughout his testimony, Savoy emphasized that his actions were taken to protect the university's server rather than for law enforcement purposes.

The federal agents obtained a search warrant from the Western District of Wisconsin, which was executed the following day. Pursuant to the warrant, the agents seized the computer and searched Heckenkamp's room.

Heckenkamp was indicted in both the Northern and South-

²They also went to the room the housing department stated was connected to the IP address ending in 117 to ensure that those records were not correct.

ern Districts of California on multiple offenses, including counts of recklessly causing damage by intentionally accessing a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(5)(B). In separate orders, Judge Ware in the Northern District and Judge Jones in the Southern District denied Heckenkamp's motions to suppress the evidence gathered from (1) the remote search of his computer, (2) the image taken of his computer's hard drive, and (3) the search conducted pursuant to the FBI's search warrant.³

The two cases were eventually consolidated before Judge Ware. Heckenkamp entered a conditional guilty plea to two counts of violating 18 U.S.C. § 1030(a)(5)(B), which allowed him to appeal the denials of his motions to suppress. The district court entered its judgment and commitment orders on April 28, 2005, and Heckenkamp filed a timely notice of appeal.

We review *de novo* both a court's denial of a motion to suppress evidence and a court's determination of whether an individual's expectation of privacy was objectively reasonable. *United States v. Bautista*, 362 F.3d 584, 588-89 (9th Cir. 2004).

II

[1] As a prerequisite to establishing the illegality of a search under the Fourth Amendment, a defendant must show that he had a reasonable expectation of privacy in the place searched. *Rakas v. Illinois*, 439 U.S. 128, 143 (1978). An individual has a reasonable expectation of privacy if he can “demonstrate a subjective expectation that his activities would be private, and he [can] show that his expectation was one that society is prepared to recognize as reasonable.”

³Judge Ware later reaffirmed his denial of the motion to suppress when Heckenkamp filed a renewed motion to suppress after the cases were consolidated.

Bautista, 362 F.3d at 589 (quoting *United States v. Nerber*, 222 F.3d 597, 599 (9th Cir. 2000)). No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of warrantless government intrusion. *Rakas*, 439 U.S. at 152-153 (Powell, J., concurring). However, we have given weight to such factors as the defendant's possessory interest in the property searched or seized, see *United States v. Broadhurst*, 805 F.2d 849, 852 n.2 (9th Cir. 1986), the measures taken by the defendant to insure privacy, see *id.*, whether the materials are in a container labeled as being private, see *id.*, and the presence or absence of a right to exclude others from access, see *Bautista*, 362 F.3d at 589.

[2] The government does not dispute that Heckenkamp had a subjective expectation of privacy in his computer and his dormitory room, and there is no doubt that Heckenkamp's subjective expectation as to the latter was legitimate and objectively reasonable. *Minnesota v. Olson*, 495 U.S. 91, 95-96 (1990). We hold that he also had a legitimate, objectively reasonable expectation of privacy in his personal computer. See *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); see also *United States v. Buckner*, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (recognizing a reasonable expectation of privacy in password-protected computer files); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (same).

[3] The salient question is whether the defendant's objectively reasonable expectation of privacy in his computer was eliminated when he attached it to the university network. We conclude under the facts of this case that the act of attaching his computer to the network did not extinguish his legitimate, objectively reasonable privacy expectations.

[4] A person's reasonable expectation of privacy may be diminished in "transmissions over the Internet or e-mail that

have already arrived at the recipient.” *Lifshitz*, 369 F.3d at 190. However, the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer. *Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001). However, privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user. *United States v. Angevine*, 281 F.3d 1130, 1134 (10th Cir. 2002); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000).

[5] In the instant case, there was no announced monitoring policy on the network. To the contrary, the university’s computer policy itself provides that “[i]n general, all computer and electronic files should be free from access by any but the authorized users of those files. Exceptions to this basic principle shall be kept to a minimum and made only where essential to . . . protect the integrity of the University and the rights and property of the state.” When examined in their entirety, university policies do not eliminate Heckenkamp’s expectation of privacy in his computer. Rather, they establish limited instances in which university administrators may access his computer in order to protect the university’s systems. Therefore, we must reject the government’s contention that Heckenkamp had no objectively reasonable expectation of privacy in his personal computer, which was protected by a screen-saver password, located in his dormitory room, and subject to no policy allowing the university actively to monitor or audit his computer usage.

III

[6] Although we conclude that Heckenkamp had a reasonable expectation of privacy in his personal computer, we conclude that the search of the computer was justified under the “special needs” exception to the warrant requirement. Under the special needs exception, a warrant is not required when

“special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.” *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (quoting *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in the judgment)). If a court determines that such conditions exist, it will “assess the constitutionality of the search by balancing the need to search against the intrusiveness of the search.” *Henderson v. City of Simi Valley*, 305 F.3d 1052, 1059 (9th Cir. 2002) (citing *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001)).

A

[7] Here, Savoy provided extensive testimony that he was acting to secure the Mail2 server, and that his actions were not motivated by a need to collect evidence for law enforcement purposes or at the request of law enforcement agents. This undisputed evidence supports Judge Jones’s conclusion that the special needs exception applied. The integrity and security of the campus e-mail system was in jeopardy. Although Savoy was aware that the FBI was also investigating the use of a computer on the university network to hack into the Qualcomm system, his actions were not taken for law enforcement purposes. Not only is there no evidence that Savoy was acting at the behest of law enforcement, but also the record indicates that Savoy was acting contrary to law enforcement requests that he delay action.

[8] Under these circumstances, a search warrant was not necessary because Savoy was acting purely within the scope of his role as a system administrator. Under the university’s policies, to which Heckenkamp assented when he connected his computer to the university’s network, Savoy was authorized to “rectif[y] emergency situations that threaten the integrity of campus computer or communication systems[,] provided that use of accessed files is limited solely to maintaining or safeguarding the system.” Savoy discovered through his examination of the network logs, in which Heck-

enkamp had no reasonable expectation of privacy, that the computer that he had earlier blocked from the network was now operating from a different IP address, which itself was a violation of the university's network policies.

[9] This discovery, together with Savoy's earlier discovery that the computer had gained root access to the university's Mail2 server, created a situation in which Savoy needed to act immediately to protect the system. Although he was aware that the FBI was already seeking a warrant to search Heckenkamp's computer in order to serve the FBI's law enforcement needs, Savoy believed that the university's separate security interests required immediate action. Just as requiring a warrant to investigate potential student drug use would disrupt operation of a high school, *see T.L.O.*, 469 U.S. at 352-53 (Blackmun, J., concurring in the judgment), requiring a warrant to investigate potential misuse of the university's computer network would disrupt the operation of the university and the network that it relies upon in order to function. Moreover, Savoy and the other network administrators generally do not have the same type of "adversarial relationship" with the university's network users as law enforcement officers generally have with criminal suspects. 469 U.S. at 349-50 (Powell, J., concurring).

[10] The district court was entirely correct in holding that the special needs exception applied.

B

Once a court determines that the special needs doctrine applies to a search, it must "assess the constitutionality of the search by balancing the need to search against the intrusiveness of the search." *Henderson*, 305 F.3d at 1059 (citing *Ferguson*, 532 U.S. at 78). The factors considered are the subject of the search's privacy interest, the government's interests in performing the search, and the scope of the intrusion. *See id.* at 1059-60.

[11] Here, although Heckenkamp had a subjectively real and objectively reasonable expectation of privacy in his computer, the university's interest in maintaining the security of its network provided a compelling government interest in determining the source of the unauthorized intrusion into sensitive files. The remote search of the computer was remarkably limited given the circumstances. Savoy did not view, delete, or modify any of the actual files on the computer; he was only logged into the computer for 15 minutes; and he sought only to verify that the same computer that had been connected at the 117 IP address was now connected at the 120 IP address. Here, as in *Henderson*, "the government interest served[] and the relative unobtrusiveness of the search" lead to a conclusion that the remote search was not unconstitutional. *Id.* at 1061.

[12] The district court did not err in denying the motion to suppress the evidence obtained through the remote search of the computer.

IV

The district court also did not err in denying the motion to suppress evidence obtained during the searches of Heckenkamp's room. Assuming, without deciding, that Savoy and the university police violated Heckenkamp's Fourth Amendment rights when they entered his dormitory room for non-law-enforcement purposes, the evidence obtained through the search was nonetheless admissible under the independent source exception to the exclusionary rule.

[13] Under the independent source exception, "information which is received through an illegal source is considered to be cleanly obtained when it arrives through an independent source." *Murray v. United States*, 487 U.S. 533, 538-39, (1988) (quoting *United States v. Silvestri*, 787 F.2d 736, 739 (1st Cir. 1986)). Therefore, we have held that "[t]he mere inclusion of tainted evidence in an affidavit does not, by itself,

taint the warrant or the evidence seized pursuant to the warrant.’” *United States v. Reed*, 15 F.3d 928, 933 (9th Cir. 1994) (quoting *United States v. Vasey*, 834 F.2d 782, 788 (9th Cir. 1987)). In order to determine whether evidence obtained through a tainted warrant is admissible, “[a] reviewing court should excise the tainted evidence and determine whether the remaining untainted evidence would provide a neutral magistrate with probable cause to issue a warrant.” *Id.* (quoting *Vasey*, 834 F.2d at 788).

[14] Here, even without the evidence gathered through the allegedly improper search, there is sufficient information in the affidavit to establish probable cause. The affidavit recited evidence that the server intrusion had been tracked “to a campus dormitory room computer belonging to Jerome T. Heckenkamp”; that “[t]he computer is in Room 107, Noyes House, Adams Hall on the University of Wisconsin-Madison”; and that “Heckenkamp previously had a disciplinary action in the past for unauthorized computer access to a University of Wisconsin system.” This was sufficient evidence to obtain the warrant to search “Room 107, Noyes House, Adams Hall.”

V

Although Heckenkamp had a reasonable expectation of privacy in his personal computer, a limited warrantless remote search of the computer was justified under the special needs exception to the warrant requirement. The subsequent search of his dorm room was justified, based on information obtained by means independent of the university search of the room. Therefore, the district courts properly denied the suppression motions.

The judgment of the district court is **AFFIRMED**.