

PETITION FOR REVIEW

PRAYER FOR REVIEW

Randal Lee Schwartz, appellant below, respectfully requests that this Court review and reverse the decision of the Court of Appeals in *State v. Randal Lee Schwartz*, 173 Or App 301, 21 P3d 1128 (2001). The Court of Appeals reversed the restitution order in part and remanded for reconsideration, and, otherwise affirmed.

QUESTIONS PRESENTED

1) Where a warrant was obtained to search defendant s home without probable cause to support the issuance of the warrant, and the police were accompanied, without court authorization, by Intel Corporation employees who were present to represent the interests of Intel and to assist in conducting the search and interrogating defendant, should defendant s statements obtained by the police officers during the execution of that search warrant be suppressed?

Did the Court of Appeals improperly analyze the exploitation test in affirming the trial court. Should the denial of the motion to controvert be reversed where the trial court made no findings of fact to support its ruling or to guide appellate court review of its decision?

2) Is the computer crime statute unconstitutionally vague either on its face or as applied? In ruling that ORS 164.377 is not vague, did the Court of Appeals misinterpret *State v. Blocker*, 291 Or 255, 261, 630 P2d 824 (1981), and apply too restrictive a test for statutory vagueness?

3) Does the copying of a password file from one Intel computer to another Intel computer, using Intel's network, and the execution of a password-guessing program on that password file also using an Intel computer, constitute theft of that password file or of the individual user's passwords?

PROPOSED RULES OF LAW

1) Where the police utilize the advantages obtained by execution of a search warrant which is not supported by probable cause to search defendant's residence and to simultaneously interrogate the defendant, any statements obtained from a defendant during the execution of that search warrant, cannot be used against the defendant, whether or not the police find other incriminating evidence during the search which might have led the police to ask questions;

2) ORS 164.377 is unconstitutionally vague in its use of the terms alter and authorization because persons to whom it is addressed cannot discern what conduct the legislature did or did not mean to prohibit and it provides no basis to distinguish socially tolerable from anti-social conduct which was intended to be prohibited;

3) The act of copying of a computer password file and the passwords from one computer to another within the same company does not constitute theft of the password file or the individual user's passwords under ORS 164.377(2)(c).

REASONS FOR REVIEW

Petitioner requests that the Court of Appeals be reversed for the following reasons:

///

1) The Court of Appeals improperly interpreted this court's holdings on exploitation in *State v. Rodriguez*, 317 Or. 27, 39-40, 854 P.2d 399; *State v. Williamson*, 307 Or 621, 626, 772 P2d 404 (1989) and *State v. Weaver*, 319 Or 212, 220-21, (and at 222, Gillette, J. concurring), 874 P2d 1322 (1994). This case presents this Court with an opportunity to clarify whether the law on exploitation prevents the use of defendant's statements obtained during an unlawful search where the police in executing a search warrant issued without probable cause, have the simultaneous purpose to seize and search defendant's home and to interrogate defendant.

The trial court, having acknowledged that some of the search warrant affidavit had been controverted, failed to specifically state what had been controverted or make any findings related to the issue of whether the facts presented by the affiant were inaccurate, untruthful or not presented in good faith. This failure has left the appellate courts without the basis necessary to determine if there was a lack of probable cause to justify the issuance of the search warrant. It appears that it is necessary to once again remind the lower courts of their obligation to make historical findings so that there is a proper record to review.

2) The computer crime statute, ORS 164.377, is unconstitutionally vague because the terms *alter* and *access* as used in the statute are impermissibly interchangeable and susceptible to different interpretations and meanings, some of which criminalize, without clear guidance or limitations, behavior which is universally accepted. Similarly, the statutory term *without authorization* is used without a standard or objective basis for determining either what *authorization* is required or the source of the *authorization*. Thus, the statute violates Article I, section 21 of the

Oregon Constitution because it "not only allow[s] a court or a jury to define a crime but to do so after the fact," and it denies due process under the Fourteenth because it does not give fair notice of what the statute proscribes. *State v. Blocker*, 291 Or 255, 260-61, 630 P2d 824 (1981). In rejecting these arguments, the Court of Appeals construed the vagueness test in *Blocker*, 291 Or at 260-61 too narrowly. By repudiating that part of its decision in *State v. Sanderson*, 33 Or App 173, 176-77, 575 P2d 1025 (1978), which stated that a statute is vague if it gives no basis to distinguish socially tolerable from anti_social conduct which was intended to be prohibited, the court leaves uncertain the appropriate test for evaluating statutes which fail to define and communicate the scope of their coverage, but which do not necessarily reach constitutionally protected conduct.

A law which is stated in terms from which those to whom it is addressed cannot discern what conduct the legislature did or did not mean to prohibit is unconstitutionally vague. *Blocker*, 291 Or at 260. Even if *Sanderson* went further than the vagueness analysis in *Blocker*, the language repudiated by the Court of Appeals should be affirmed by this Court. In so doing this Court would clarify that gray area between the reach of a statute which is clear but overbroad because it reaches constitutionally protected acts, and a law which can reach even undeniably innocuous or socially acceptable conduct because the terms of the statute are too elastic and susceptible to *ad hoc* definition.

3) Defendant's assignment of error that the trial court should have granted the defendant's Motion for Judgment of Acquittal on Counts 2 and 3, which charged

violations of ORS 164.377(2)(c)¹, because nothing was taken, appropriated, obtained or withheld from Intel Corporation when defendant copied the password file from one Intel computer to another Intel computer, raises questions of first impression for this Court as to the statutory construction of ORS 164.377, the computer crime statute. The issue requires the court to construe the meaning of the term theft as it is used in, whether the definition of theft in ORS 164.015 applies to that statute, and if so, the meaning of take in ORS 164.015. The state's argument, that by copying passwords, defendant stripped them of their value, actually describes conduct which damages the value of property but does not constitute a taking, appropriation or withholding of property.

Schwartz, 173 Or App at 316-17. That conduct describes the crime of criminal mischief rather than theft; it is not covered by the computer crime statute. The Court of Appeals interpretation that theft as used in ORS 164.377(2)(c) could be established by showing an act of obtaining control of property was reached by defining the term take beyond common application without the benefit of controlling authority. The court's definition did not address defendant's argument that his conduct did not constitute theft and did not fit under the statute. 173 Or App at 317. By addressing this question of first

¹ (2) Any person commits computer crime who knowingly accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of:

* * * *

(c) Committing theft, including, but not limited to, theft of proprietary information.

In pertinent part, ORS 164.015 defines "theft" as follows:

A person commits theft when, with intent to deprive another of property or to appropriate property to the person or to a third person, the person: (1) Takes, appropriates, obtains or withholds such property from an owner thereof; . . .

impression, this Court will provide guidance as to the proper construction of the computer crime statute.

STATEMENT OF FACTS²

Defendant worked as an independent contractor for Intel Corporation beginning in the late 1980s. Defendant's tasks included programming, system maintenance, installing new systems and software, and resolving problems for computer users. At various times, including at the time of the events in question, defendant performed the duties of a systems administrator. (7-13-95 Tr. 106-107; 7-21-95 Tr. 151). In late 1991 or early 1992, defendant began working in Intel's Supercomputer Systems Division (SSD). SSD creates large computer systems that can cost millions of dollars and are used for applications such as nuclear weapons safety. Intel considers the information stored on its SSD computers to be secret and valuable. Each person using SSD computers must use a unique password in order to gain access to electronic information stored there. Passwords are stored in computer files in an encrypted or coded fashion.³

²This statement of facts supplements the facts set out in the opinion of the Court of Appeals, *Schwartz*, 173 Or App at 303-305, which are restated for purposes of continuity and ease of reading. Since the record of pretrial and trial proceedings are not uniformly paginated, references to the record show the date of the proceeding followed by "Tr" and the specific page numbers.

³ Passwords are groups of computer characters, usually letters, digits and printable punctuation which, when used in conjunction with the applicable "username," permit access to the information stored on a computer or group of computers. (7-13-95 Tr. 178, 181). They are "encrypted (7-13-95 Tr. 179)," using a mathematical formula known as an "algorithm," and kept in a file on the computer. Anyone with access to the computer can see the password file. (7-18-95 Tr. 95). To gain access to the computer and its files, a user must "login" with a username and the unencrypted counterpart to that specific user's password. (7-18-95 Tr. 7). The computer, using the "algorithm," encrypts the password which is offered, and then compares it to the password listed for

In the spring of 1992, defendant and Poelitz, an Intel systems administrator, had a disagreement about how defendant had handled a problem with SSD's e_mail system. The problem was ultimately resolved in an alternative manner suggested by Poelitz, which upset defendant and made him believe that any future decisions he made would be overridden. Accordingly, defendant decided to terminate his SSD contract with Intel. As defendant himself put it, he "hadn't left SSD on the best of terms." At that time, his personal passwords onto all but one SSD computer were disabled so that defendant would no longer have access to SSD computers. His password onto one SSD computer, Brillig, was inadvertently not disabled.

After defendant stopped working with SSD, he continued to work as an independent contractor with a different division of Intel. In March 1993, Brandewie, an Intel network programmer and systems administrator, noticed that defendant was running a "gate" program on an Intel computer called Mink, which allowed access to Mink from computers outside of Intel. "Gate" programs like the one defendant was running violate Intel security policy, because they breach the "firewall" that Intel has established to prevent access to Intel computers by anyone outside the company. Defendant was using the gate program to use his e_mail account with his publisher and to get access to his Intel e_mail when he was on the road. Brandewie talked to defendant about his gate program's security, and even though defendant believed that

that user in the password file. If it matches, the user is given access to the computer and/or the system.

precautions he had taken made his gate program secure, he agreed to alter his program. (7-21-95 Tr. 129).

In July 1993, Brandewie noticed that defendant was running another gate program on Mink. This program was similar to the earlier gate program and had the same effect of allowing external access to Intel computers. Defendant protested that changes he had made to the program made it secure, but Brandewie insisted that defendant remove the program or get authorization to run it from corporate security. At that point, defendant decided that Mink was useless to him without a gate program, so he asked that his account on that computer be closed. Defendant then moved his gate program onto an Intel computer called Hermes. Because that computer was too slow for him, defendant finally moved his gate program onto the SSD computer Brillig.

In the fall of 1993, defendant downloaded from the Internet a program called "Crack," which is a sophisticated password guessing program.⁴ Defendant began to run the Crack program on password files on various Intel computers.⁵ When defendant ran the Crack program on Brillig, he learned the password for "Ron B.," one of Brillig's authorized users. Although he knew he did not have the authority to do so, defendant

⁴ The password cracking program is freely available on the internet, (6-14-95 Tr. 188), and is used by system administrators to insure the effectiveness of password files. (7-13-95 Tr. 127); (7-14-95 Tr. 91; 212); (7-19-95 Tr. 63). It uses the algorithm to encrypt words and their derivations from a dictionary or dictionaries available to it. (6-14-95 Tr. 188); (7-14-95 Tr. 178). Then it compares the encrypted word to the encrypted passwords in the password file. (7-13-95 Tr. 179); (7-20-95 Tr. 140, 142). If it comes up with a match, the password is "cracked" and the system administrator notifies the user to change his or her password. (7-13-95 Tr. 105). Intruders, if they are able to gain access to the system, may also use such a program to "crack" one or more passwords and then use the cracked password(s) to gain access to the information to which that user has access. (7-13-95 Tr. 137).

then used Ron B.'s password to log onto Brillig. From Brillig, he copied the entire SSD password file onto another Intel computer, Wyeth. Once the SSD password file was on Wyeth, defendant ran the Crack program on that file and learned the passwords of more than 35 SSD users, including that of the general manager of SSD. Apparently, defendant believed that, if he could show that SSD's security had gone downhill since he had left, he could reestablish the respect he had lost when he left SSD. Once he had cracked the SSD passwords, however, defendant realized that, although he had obtained information that would be useful to SSD, he had done so surreptitiously and had "stepped out of my bounds." Instead of reporting what he had found to anyone at SSD, defendant did nothing and simply stored the information while he went to teach a class in California.

After he returned from California, defendant decided to run the Crack program again on the SSD password file, this time using a new, faster computer called "Snoopy." Defendant thought that, by running the Crack program on the SSD password file using Snoopy, he would have "the most interesting figures" to report to SSD security personnel.⁶

On October 28, 1993, Mark Morrissey, an Intel systems administrator, noticed that defendant was running the Crack program on Snoopy. The password cracking

⁵This was a common practice among systems administrators.

⁶ Network security is a major concern for companies such as Intel (7-14-95 Tr. 98), because the engineers and scientists work on the network, and their work is considered a company secret. (7-13-95 Tr. 102-103). It is part of the job of a systems administrator to see to it that the systems which he/she administers are secure against such intrusions. (7-13-95 Tr. 102). At the time he ran the password cracking program, defendant was an independent contractor at Intel with system administrator duties involving the operation of Intel's email systems. (7-13-95 Tr. 106-107; 7-21-95 Tr. 151).

program was running under defendant's own username and password (6-14-95 Tr. 187; 7-14-95 Tr. 168). At that point, Morrissey contacted Richard Cower, an Intel network security specialist, for advice about how to proceed. In investigating defendant's actions, Morrissey realized that defendant had been running a gate program on the SSD computer Brillig, even though defendant's access should have been canceled.

On October 29, 1993, Intel staff met to discuss the situation, and because defendant was out of town it was decided to do nothing until Monday. (6-13-95 Tr. 80-81; 7-14-95 Tr. 136). A suggestion was made that it might be advantageous to simply ask defendant what was going on when he returned. The idea was vetoed by someone in authority who said that the decision to prosecute defendant had already been made. (7-14-95 Tr. 225-226; 7-18-95 Tr. 148) and the police were contacted.

On the morning of Monday, November 1, 1993, Cower, Morrissey, John Kent, systems administrator for the SSD division, Clyde Stites, Intel security specialist, Richard Pierce, in-house counsel, and paralegal Janice Baldwin met with Detectives Lilley and Lazenby of the Washington County Sheriff's office and DDA Thomas Tintera. (9-20-94 Tr. 77-78). An affidavit in support of a warrant to search defendant's home was then prepared.⁷

Later on November 1, 1993, the search warrant was executed at defendant's residence. In addition to some uniform officers, the detectives in charge of the case invited Intel employees, Cower, Pierce, and Stites along to help execute the warrant (9-20-94 Tr. 80-81). Det. Lilley testified that the Intel people were invited along to assist

⁷See appellant's opening brief, App. 1-5.

him in understanding defendant's answers to his questions, to help identify items of evidentiary value, to assist in maintaining the integrity of that evidence and to safeguard against damage to the computers so that the police would not get sued. (9-20-94 Tr. 80-81).⁸

At one point, Cower was asked to look at a Macintosh computer that was downloading files, and he told the officers that "it looked okay to [him]." (9-20-94 Tr. 102). His other involvement was to participate in the interrogation of defendant for an aggregate time of about one hour. (9-20-94 Tr. 103).

Pierce accompanied the officers, first and primarily, in order to represent Intel Corporation, to "fire" defendant and to terminate his access to any Intel buildings. (9-20-94 Tr. 136). Second, Pierce was there to identify, on behalf of Intel Corporation, the "assets" that might be located on diskettes or running on a computer screen somewhere. (9-20-94 Tr. 136-37). Stites went along to collect the badges that Intel had issued to defendant. (9-20-94 Tr. 101). Pierce and Stites were present during the interrogation for a very brief period of time. (9-20-94 Tr. 105).

During the search, defendant's two laptop computers and two hard drives were seized and examined by one of the two Washington County Deputy Sheriffs trained in computer evidence analysis. (7-19-95 Tr. 96-97). The data stored on Defendant's computers was examined using technology which makes a "mirror copy" of the data in those devices. (7-19-95 Tr. 98). This mirror copy preserves not only whole, active files

⁸ Det. Lazenby was trained in procedures to secure computers and safeguard data in the computers. (6-13-95 Tr. 69). Thus, no one from Intel was needed to help safeguard the information on the computers.

but also bits and pieces of files that have been erased but not overwritten.⁹ (7-19-95 Tr. 98).

The data in the mirror image then was searched using a program that looks for keywords.¹⁰ (7-19-95 Tr. 98-99). After that, the data was searched for anything of evidentiary value. (7-19-95 Tr. 99). This process was completed four times, one for each device. (7-19-95 Tr. 99). Nothing of an incriminating nature was found on either of the hard drives or on either of Defendant's laptop computers. (6-15-95 Tr. 286; 7-14-95 Tr. 228; 7-19-95 Tr. 103).

During the execution of the warrant, Det. Lilley interviewed Defendant for two hours. (6-15-95 Tr. 50). Lilley's understanding of computers was very limited. (7-13-95 Tr. 61). He did not understand much about what Defendant had to say.¹¹ (7-13-95 Tr. 45). Small portions¹² of the conversation were recorded in his notes and included in his police report. (6-15-95 Tr. 42-50). According to Det. Lilley, his report was "the summary of the essence of what was said." (7-13-95 Tr. 76).

Defendant, seeking suppression of his statements, filed both a Motion to Suppress and a Supplementary Motion to Suppress. The Supplementary Motion to

⁹The mirror imaging technology does not work on laptops, so the data was copied from the laptops to another hard drive prior to the examination. (7-19-95 Tr. 104).

¹⁰The keywords were supplied by Intel and the printouts of the results of the keyword searches were presented to Intel. (7-19-95 Tr. 100-101).

¹¹For example, Det. Lilley understood Defendant to say that "root" is a program which is "the means for which he ran the Crack program." (7-13-95 Tr. 81, 83). "Root" is a term that designates a system administrator's privilege in a network of computers using the UNIX operating system, not a program. (6-14-95 Tr. 179; 7-13-95 Tr. 135). One with "root" access can do anything on that system. (7-13-95 Tr. 134-135).

Suppress sought to controvert "the good faith, accuracy and truthfulness of the affiant" * * ." ORS 133.693(1) and the Motion to Suppress challenged the sufficiency of the affidavit to support issuance of the warrant.¹³ The trial court acknowledged that parts of the affidavit had been controverted, refused to make any findings of fact or render any conclusions of law respecting that, and* denied the motions. The Court of Appeals affirmed.

ARGUMENT

A. Suppression of Defendant s Statements. Exploitation Analysis.

In the Court of Appeals, defendant argued that statements obtained from him during the execution of a defective warrant to search his home should have been suppressed as the fruit of an illegal search. He based that challenge on the following four grounds: 1) a motion pursuant to ORS 133.693(1) to controvert the "good faith, accuracy and truthfulness of the affiant" whose statements led to the issuance of the search warrant; 2) the facts in the affidavit supporting the warrant were insufficient to support probable cause; 3) the warrant was overly broad; and, 4) the warrant was executed in violation of ORS 133.575. The Court of Appeals did not address the substance of the forgoing challenges because it determined, assuming that the warrant or its execution were defective, that suppression of defendant's statements is not

¹²Det. Lilley's testimonial rendition of his two-hour long conversation with Defendant, including questions by the prosecutor, took 15 minutes. (7-13-95 Tr. 75-76).

¹³Because the Court of Appeals did not rule on whether the motions to controvert and suppress should have been granted, petitioner has not included the facts relevant to those issues in this petition for review. Instead, he relies on the additional facts pertaining to those assignments of error in his brief in the Court of Appeals.

warranted, because the statements were not obtained by exploitation of the search.

Schwartz, 173 Or App at 307.¹⁴

As a preliminary matter, there are at least two reasons why the trial court was in error when it refused to conduct the required analysis of the challenged affidavit. First, ORS 133.693 requires that it do so. Second, the trial court's failure to make the requisite findings with respect to the controverted affidavit deprived the reviewing court of the record that it needs to make a reasoned decision whether ruling below was correct.¹⁵ This error, alone, is an adequate basis for reversing the trial court's ruling. See, *State v. Wise*, 305 Or 78, 81-82 and n. 2, 749 P2d 1179 (1988).

1. The trial court's failure to comply with the statute was erroneous.

ORS 133.693 provides in relevant part:

(1) Subject to the provisions of subsection (2) of this section, in any proceeding on a motion to suppress evidence the moving party shall be entitled to contest, by cross-examination or offering evidence, the good faith, accuracy and truthfulness of the affiant with respect to the evidence presented to establish probable cause for search or seizure.

*

*

(5) The court shall determine whether, under applicable law, any inaccuracy, untruthfulness or lack of good faith requires suppression.

The sections of the statute quoted require that the trial court analyze the affidavit. *State v. Harp*, 299 Or 1, 697 P.2d 548 (1985). A judge subtracts from the affidavit all of those portions of it that are untrue or inaccurate and then determines if what is left

¹⁴Defendant relies on those facts and arguments set out in the First Assignment of Error in his brief in the Court of Appeals at pp 3-37.

¹⁵In both the caption and the body of his Supplementary Motion to Suppress, defendant requested "Specific Findings of Fact and Conclusions of Law." The trial court simply found that "[A]ny omissions or inaccuracies" were not material. It did not find that there

amounts to probable cause. 299 Or at 9. Of course, the defendant must first show that there is a substantial basis for challenging the affidavit. *Id.* at 10. If he does so, then the court reviewing the affidavit must assess it independently of the magistrate's decision. *Id.* at 11. ORS 133.693(5) deprives a trial court of any discretion not to make that analysis.

In the present case, defendant identified a number of inaccuracies, untruths and omissions in the affidavit¹⁶. Once he had done so, the trial court was required to conduct the analysis and provide the Court of Appeals with a list of the assertions in the search warrant affidavit that it deemed to be inaccurate. *Wise*, 305 Or at 81-82 and n. 2; *State v. Bates*, 304 Or 519, 527-28, 747 P2d 991 (1987); *State v. Dimeo*, 304 Or 469, 478 n. 4, 747 P2d 353 (1987). In the present case it did not do so and that was error.

2. The trial court's failure to make historical findings was erroneous.

This Court has long and repeatedly required that trial courts make findings of historical fact. *Ball v. Gladden*, 250 Or 485, 487, 443 P.2d 621 (1968). Such findings are necessary so that the reviewing court can make its decision on whether the trial court correctly followed the law. A recent example of such a process is found in *State v. Keeney*, 323 Or 309, 918 P.2d 419 (1996). Unfortunately, the Court has had to remind lower courts, from time to time, of their obligation to make the historical findings. *Dimeo*, 304 Or at 479 n. 4;

were no such omissions or inaccuracies. In fact, the trial court noted on the record that there were both inaccuracies in, and omissions from, the affidavit. (6-15-95 Tr. 285-6).

¹⁶Those errors are set forth in defendant's brief in the Court of Appeals briefs at pp 13-24. He relies on those arguments and will not repeat them here.

In the present case, the trial court failed to make any findings related to the issue of whether the affiant was inaccurate, untruthful or not in good faith. Such a failure has left this Court without the findings that it needs in order to determine if there was a lack of probable cause to justify the issuance of the search warrant. It appears that is necessary to once again remind the lower courts of their obligation to make historical findings so that there is a proper record to review. *Wise*, 305 Or at 81-82 (The Court stated at n. 2: These supplications seem to have fallen on deaf ears; henceforth, the Court of Appeals should not hesitate to send cases back to the trial courts for requisite findings of historical fact when trial courts fail in their obligations.).

3. The conclusion that the police did not exploit the illegal search was erroneous.¹⁷

The Court of Appeals simply decided that even if the warrant to search defendant s home or the execution of that warrant were defective, it did not make any difference because there was no exploitation arising from the execution of the search warrant. It reasoned that since nothing was found in the search, and the police would have interviewed defendant regardless of what the search produced, there was no exploitation. 173 Or App at 307-08. That reasoning overlooked the interrelationship between the role of the search of the home, the way that it was executed and the contemporaneous interrogation of defendant.

First, the police were entitled to be at the residence only because they were clothed with the authority of a search warrant. Of course, [t]he security of the home is the ultimate objection of all government and it is the obligation of the courts to enforce

the state and federal constitutional provisions intended to protect the individual in the sanctity of his home. *State v. Duffy*, 135 Or. 290, 297, 295 P.953 (1931). The right of a person to retreat into his own home and there be free from unreasonable governmental intrusion stands at the very core of the Fourth Amendment. *Kyllo v. United States*, 121 SCt 2038 (2001). Consequently, government officials, in executing a search warrant on a person's home, must ensure that the search is conducted in a way that minimizes unwarranted intrusions into a person's privacy.

Here, the issuance of the defective search warrant provided the justification for the police presence in and in total control of defendant's home, its possessions and his person. Second, that warrant allowed that most private of places to be invaded not only by various police officers but by employees of Intel, whose presence, under the circumstances of the case, violated ORS 133.575.¹⁸ The magistrate who issued the warrant did not authorize the police to employ the assistance of the civilians employees, despite the fact that the same three employees were involved in the preparation of the affidavit and the magistrate's permission could have been sought. Some of those Intel employees were admittedly brought by the police to assist in the execution of the search and, notably, in the pre-planned, contemporaneous questioning of defendant. (9-20-94 Tr. 69¹⁹; 80-81). Other Intel personnel were present to represent the interests of Intel

¹⁷Defendant also relies on the authority cited and his arguments on exploitation in his reply brief in the Court of Appeals at pp 6-10.

¹⁸See appellant's opening brief at pp 34-37.

¹⁹ Detective Lilley testified that he had explained to Defendant that the Intel employees were there to help the detective understand Defendant's answers. He did not testify that he gave Defendant any choice in the matter.

Corporation and conducted company business while the warrant was executed. (9-20-94 Tr. 136).

The fact pattern at issue is unlike most exploitation cases. Usually, the police make an illegal stop and then conduct a search in which evidence is found which then must be suppressed. See, e.g., *State v. Williamson*, 307 Or 621, 626, 772 P.2d 404 (1989)(defendant stopped at unlawful roadblock); *State v. Valdez*, 277 Or 621, 651 P.2d 1006 (1977)(stop and frisk without reasonable suspicion). Or the police are unlawfully present in a location and find physical evidence. *State v. Hansen*, 295 Or 78, 664 P.2d 1095 (1983)(unlawful entry into residence on suspicion defendant had marijuana).

In the present case the defendant contends that the police were unlawfully present in his home, because the search warrant was issued without probable cause, and they employed unauthorized civilian personnel to assist in both the search of defendant's home and in his interrogation. That was done by prearrangement -- the interrogation of defendant was one of the principal aims of the execution of the search warrant. The police and Intel employees co-operated in obtaining the warrant and coordinated the execution of the warrant.

Here, the police utilized the resulting advantage gained by the search and seizure of defendant's home and person to obtain statements from him, even if the search did not produce incriminating evidence or other information which caused the police to ask defendant questions. This is so, notwithstanding the possibility that the police would have desired to interview defendant anyway.

It is not just that the police were merely present in his home to search unlawfully. They also were there for the purpose of interrogating defendant, using the Intel

employees to obtain incriminating statements from defendant. In effect, they were intruders who occupied Defendant's home and in that highly intimidating setting leveraged their presence to obtain the statements. Nor does it matter that the police had already focused their attention on Defendant; of course, they did since they had a search warrant.

The police were able to conduct the interview under those charged circumstances only because they took advantage of a search warrant that they were not entitled to have to take command of defendant's home and person. They utilized Intel employees whose presence had not been authorized by a court and who took advantage of their presence during the search to conduct Intel business. These facts demonstrate that the execution of the search warrant and interrogation of defendant were inseparably linked under the circumstances.

In short, the police took advantage of the circumstances of their unlawful conduct when they obtained the statements from defendant that were used against him at trial. *State v. Rodriguez*, 317 Or. 27, 39-40, 854 P2d 399 (1993)(Evidence obtained during a later consent search should be suppressed only in those cases where the

police have exploited their prior unlawful conduct to obtain the consent. Exploitation occurs when the police take advantage of the circumstances of their unlawful conduct).

The Court of Appeals holding that the police did not exploit their unlawful conduct, if any occurred, misapplied legal principles governing circumstances when evidence must be suppressed because it is the fruit of prior police misconduct.

Resolution of the issues raised implicates state statutes and the search and seizure

provisions of the state and federal constitutions. Consequently, the Court should take this opportunity to give a definitive interpretation of how and when civilian involvement in the execution of a search is authorized under ORS 133.575 and to clarify the law on exploitation particularly in circumstances, as here, where the unlawful police conduct occurs in the home and is inextricably intertwined with the contemporaneous interrogation of the defendant which produced the contested evidence.

B. ORS 164.377, the computer crime statute, unconstitutionally vague. The Court of Appeals misinterpreted *State v. Blocker*, 291 Or 255, 261, 630 P2d 824 (1981) and applied too restrictive a test for statutory vagueness.

ORS 164.377, is unconstitutionally vague²⁰ because the terms alter and access as used in the statute are impermissibly interchangeable and susceptible to different interpretations and meanings without clear guidance or limitations. Similarly, the statutory term without authorization contains standard or objective basis for determining either what authorization is required or the source of the authorization.

In rejecting these arguments, the Court of Appeals erroneously construed the vagueness test in *Blocker*, 291 Or at 260-61 too narrowly. It reads *Blocker* to limit appellate court scrutiny of the reach of statutes to the doctrine of unconstitutional overbreadth. *Schwartz*, 173 Or App at 311-12. According to the Court of Appeals interpretation of *Blocker*, if a statute does not expressly prohibit constitutionally protected conduct, it cannot by definition reach too far, and if it does so it is unconstitutionally overbroad but not unconstitutionally vague. 173 Or.App. at 312.

²⁰The statute violates Article I, section 21 of the Oregon Constitution and the due process clause of the Fourteenth Amendment to the United States Constitution.

This interpretation fails to consider this Court's holdings that the vice of a statute which is unconstitutionally vague is that its terms fail "to define and communicate its coverage[.]" *State v. Robertson*, 293 Or 402, 411, 649 P2d 569 (1982). A statute which is overbroad reaches constitutionally protected behavior as a matter of law. On the other hand, a vague statute may reach constitutionally protected or socially acceptable behavior depending on how it is interpreted on an *ad hoc* basis. Its coverage is so elastic that it "permits the judge and jury to punish or withhold punishment in their uncontrolled discretion[.]" *State v. Hodges*, 254 Or 21, 27, 457 P2d 491 (1969).

Thus, it is a characteristic of a vague statute that it does, at least in certain circumstances, cover too much ground. That is where the doctrine of vagueness and the doctrine of overbreadth intersect. That intersection is a significant one, with far-reaching implications. The Court of Appeals' opinion in this case removes an important guidepost for evaluating statutes which cross that intersection.

In this case, the defense focused on the statutory terms "alter"²¹ and "access,"²² arguing that they were unconstitutionally vague in that their respective terms embraced both criminal conduct and conduct that was completely innocuous²³ and, second, that their meanings were impermissibly interchangeable and susceptible to a host of different possible interpretations of meaning.

²¹This is the operative statutory term in Count 1 of the indictment, which alleged a violation of ORS 164.377(3)

²²This is the operative statutory term in Counts 2 and 3 of the indictment, which alleged violations of ORS 164.377(2)(c).

²³The state had admitted that the statutory term "alter" could mean something as simple as changing the color on a computer screen. 7/1/94 Tr. 27 l. 25 - Tr. 28 l. 4. The defense established that virtually anything one does to a computer alters it within the meaning of the statute. 7/14/95 Tr. 128-129, Tr. 140 ll. 23-25.

In effect, the Court of Appeals determined that it was permissible for the legislature to enact legislation criminalizing conduct that is both reprehensible and conduct that is universally accepted as socially tolerable and fail to draw any statutory boundary between the two, leaving that task to judges and juries.

In order to reach that conclusion, the Court of Appeals expressly disavowed its own language in one of its own precedents: In *State v. Sanderson*, 33 Or App 173, 575 P2d 1027 (1977), the court held that a statute which prohibited "Engag[ing] in a course of conduct that alarms or seriously annoys another person and which serves no legitimate purpose" was unconstitutionally vague because it provided no basis to distinguish between socially tolerable conduct, e.g., consistently appearing late for social appointments, and the antisocial conduct intended to be prohibited, such as the making of obscene telephone calls. 33 Or App at 176-177.

There were two fatal flaws in the quoted statutory language as the Court of Appeals saw it in *Sanderson*: "The over_generality of the language and its subjective quality." 33 Or App at 177. What was missing was "language providing guidance for even application, [which meant that] the parameters of the criminal conduct defined by the statute are so elastic that the judicial determination of guilt or innocence in each individual prosecution must necessarily be ad hoc, unregulated by legislative standards." Considering whether a limiting construction could save the statute, the court said: ". . . it appears that the legislature used deliberately general language to create a statute elastic enough to encompass a wide range of undefined conduct. It succeeded all too well." *Id.*

Both the rule of *Sanderson*, and its rationale, should be upheld by this Court.

They are good law, and they are consistent with this Court's jurisprudence on the vagueness doctrine. They amplify and clarify the rule that:

"Vagueness" means that a penal law is stated in terms from which those to whom it is addressed potential defendants, prosecutors, courts, and jurors cannot discern what conduct the lawmaker did or did not mean to include in the prohibition. Such a failure of communication in penal laws has been held to contravene Article I, section 21 of the Oregon Constitution because "they not only allow a court or a jury to define a crime but to do so after the fact," [citations omitted] [291 Or. 261] and to deny due process under the Fourteenth Amendment because they do not give fair notice of what they proscribe. *State v. Blocker*, 291 Or. 255, 260-261, 630 P.2d 824 (1981).

The fact that the statute in this case addresses itself to a virtually unlimited range of conduct respecting computers -- to do anything whatever to a computer alters it -- much of which is completely innocuous, is the key to its unconstitutional vagueness. It allows employers, judges and juries to determine, **after the conduct occurs**,²⁴ whether or not it was criminal. *See also, State v. Robertson*, 293 Or 402, 411, 649 P2d 569 (1982) (the vice of a statute which is unconstitutionally vague is that its terms fail "to define and communicate its coverage[.]").

The same problem exists with respect to the term "authorization" in ORS 164.377: The statute contains no standards for the determination, on any objective basis, of what sort of "authorization" is required, nor does it identify the source from which the authorization must originate. The latter omission distinguishes ORS

²⁴The "alterations" that were the subject of Counts 1 and 2 occurred and were corrected in about March, 1993. They were not deemed, at the time, to be important enough to be reported to management. However, in November, 1993, after the Vice-President's password had been cracked, they became felonies.

164.377(3) from virtually every other section of the Oregon Revised Statutes where the term "authorization" is used to mean "permission."²⁵

This case provides a paradigm example of why this term in this statute, without modifiers, is unconstitutionally vague. Defendant answered directly to Robert Wilcox. (7-13-95 Tr. 94, 101-102). Defendant was hired to monitor computer networks with UNIX workstations. This required an expert; Wilcox, was not an expert in that area and Defendant was. (7-13-95 Tr. 94-95, 123-24).

The inevitable consequence was that none of the changes (read alterations) wrought by Defendant in the ordinary course of his employment were "authorized" by anyone. He was hired by his supervisor for his expertise; expertise which the supervisor did not possess. Wilcox **relied** on Defendant's expertise. (7-13-95 Tr. 124). In fact, Wilcox made it clear that **it is the systems administrators themselves** who know what is to be done and not to be done. (7/13/95 Tr. 102). Therefore, the systems administrators "authorized" whatever they did as they did it. Nothing they did was ever authorized in advance.

The Court of Appeals asserted that, in this case, "defendant himself acknowledged that installing gate programs was against company policy[,] 173 Or App at 313. However, that statement misinterprets the record. When he first testified, Defendant said that Mr. Brandewie²⁶ and Mr. Morrissey had told him that the gate program was not secure enough. (7-21-95 Tr. 129). Brandewie agreed. (7-18-95 Tr. 36). There was never any testimony that anyone informed Defendant that installing

²⁵Appendix A to Defendant's Demurrer in the trial court sets out the exhaustive list of statutory references to the term authorization.

such a program²⁷ was against company policy before he installed the first one. In fact, Defendant had been directed to create a working port reflector²⁸ when he worked as a system administrator at IWARP.²⁹ (7-19-95 Tr. 123-124).

Brandewie testified that his computer system's security arrangements were based on Intel policy **as he understood it**. (7-18-95 Tr. 42). Thus, when he was talking to Defendant about security policy, what he said had only to do with **his** computers. He had no idea whether policy manuals had been distributed to other employees, much less independent contractors. (7-18-95 Tr. 43). Having agreed with Brandewie's assessment of the program, Defendant changed it. (7-21-95 Tr. 129-130). He testified that he believed, afterward, that the program complied with company policy and he explained why. (7-21-95 Tr. 132-133).

Rich Cower, Intel Security, expressed doubt that any policy manuals had been distributed to independent contractors. (7-18-95 Tr. 173). Morrissey testified in another context that the methods used by Intel were, to a very large extent, "ad hoc" and do not fully "close the loop." (7-14-95 Tr. 215). In fact, it was generally against company policy, i.e., "unauthorized," for independent contractors to be system administrators. (7-18-95 Tr. 64-65). That policy was, up to and including the time of the trial, routinely ignored. Defendant worked as a system administrator there for years, a circumstance

²⁶Brandewie was Mink's administrator.

²⁷Defendant experimented with several gate programs, each one more sophisticated, in an effort to create one that would work acceptably to Mr. Brandewie. (7-21-95 Tr. 132-138).

²⁸A program that would accept internet connections from outside of Intel. The "gate" program was a port reflector, according to Brandewie. (7-18-95 Tr. 11).

²⁹One of the divisions that eventually became part of SSD. (7-19-95 Tr. 121) (testimony of James Reinders).

that the Information Technology Manager at SSD saw as a fundamental violation of company policy. (7-18-95 Tr. 65). Thus, from his point of view, Defendant's employment by Intel was "without authorization." Yet Intel routinely paid the bills Defendant sent, and Intel routinely accepted the fruits of his labor.

Under these circumstances, the terms "authorization" and "alter" as used in the computer crime statute, fall well within that select group of terms in penal statutes that have been shown to exhibit "no [discernable] standard of conduct * * * at all" because of their impermissible generality. *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 US 489, 494_95, 102 SCt 1186, 1191_92, 71 LEd2d 362 (1982) quoting *Coates v. City of Cincinnati*, 402 US 611, 614, 91 SCt 1686, 1688, 29 LEd2d 214 (1971); and see, *State v. Chakerian*, 325 Or 370, 381-2, 938 P2d 756 (1997); *Robertson*, 293 Or at 411; *Blocker*, 291 Or at 260-61 (a law which is stated in terms from which those to whom it is addressed cannot discern what conduct the legislature did or did not mean to prohibit is unconstitutionally vague).

C. Copying password files and passwords did not constitute theft under ORS 164.377(2)(c). Defendant's Motion for Judgment of Acquittal should have been granted.

In order to find that there was evidence to support defendant's conviction, the Court of Appeals had to define theft as it applies to ORS 164.377(2)(c). The court referred to the definition of theft in ORS 164.015. This, in turn, required the court to define the meaning of take in that statute. The court considered various dictionary definitions and concluded that the term take

. . . might include more than just the transfer of exclusive possession that defendant proposes. For example, "take" could include obtaining control

of property, as defendant did with respect to the passwords and password file by copying them. 173 Or App at 317.

Thus, under this definition, the act of copying a file can be a theft.

Defendant contends that the trial court should have granted the Motion for Judgment of Acquittal on Counts 2 and 3, which charged violations of ORS 164.377(2)(c)³⁰, because nothing was taken, appropriated, obtained or withheld from Intel Corporation when defendant copied the password file from one Intel computer to another Intel computer. This claim raises questions of first impression for this Court as to the construction of ORS 164.377, the computer crime statute. The issue requires the court to construe the meaning of the term theft as it is used in, whether the definition of theft in ORS 164.015 applies to that statute, and if so, the meaning of take in ORS 164.015.. The state s argument, that by copying passwords, defendant stripped them of their value, actually describes conduct which damages the value of property but does constitute a taking, appropriation or withholding of property. *Schwartz*, 173 Or App at 316-17. That conduct describes the crime of criminal mischief rather than theft; it is not covered by the computer crime statute.

³⁰ (2) Any person commits computer crime who knowingly accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of:

* * * *

(c) Committing theft, including, but not limited to, theft of proprietary information.

In pertinent part, ORS 164.015 defines "theft" as follows:

A person commits theft when, with intent to deprive another of property or to appropriate property to the person or to a third person, the person: (1) Takes, appropriates, obtains or withholds such property from an owner thereof; . . .

The Court of Appeals determined that theft as used in ORS 164.377(2)(c) could be established by evidence of an act of obtaining control of property. This result was reached by defining the term take in ORS 164.015 to cover a range of activity beyond its common application to include acts where someone has a copy of something, but, does not have possession of the property itself. This interpretation was reached without the benefit of controlling authority. It improperly expands the terms of the statute in violation of the injunction against courts including in a statute what has been omitted. ORS 174.010.

The Court of Appeals also failed to address defendant's argument that his conduct of copying files did not fit under the statute because the evidence did not show he had the intent to deprive another of property, or to appropriate the property to himself. 173 Or App at 317.

By addressing this question of first impression, this Court will provide guidance as to the proper construction of the computer crime statute.

IMPORTANCE OF ISSUES

This case presents a significant issue concerning the interpretation of constitutional provisions and the law of exploitation of unlawful police conduct. It also presents questions of first impression concerning the constitutionality of ORS 164.377, the computer crime statute, and the interpretation of various provisions of that statute.

CONCLUSION

For all these reasons, defendant respectfully requests that this Court grant review of his case and reverse the decision of the Court of Appeals.

Respectfully submitted,

MARC SUSSMAN OSB #77368
Attorney for Randal Lee Schwartz
Defendant-Appellant
Petitioner on Review

CERTIFICATE OF SERVICE

I certify that on October 10, 2001, I served two certified copies of the forgoing *PETITION FOR REVIEW* by mailing them to: Mr. Michael D. Reynolds, Solicitor General, Appellate Division, Department of Justice, 1162 Court Street NE, Salem, Oregon 97310.

Dated this 10th day of October, 2001.

Marc Sussman, OSB #77368
Attorney for Defendant-Appellant
Petitioner on Review